1924.70199 PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In Re U.S. Patent Application)
)
Applicant: Omote et al.)
)
Serial No.)
)
Filed: March 30, 2004)
)
For: DEVICE AND METHOD FOR WORM DETECTION, AND COMPUTER PRODUCT)
)
Art Unit:)

I hereby certify that this paper is being deposited with the United States Postal Service as EXPRESS MAIL in an envelope addressed to: Mail Stop PATENT APPLICATION, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450, on this date.

March 30, 2004 *Express Mail Label No.: EV032736278US*
Date

CLAIM FOR PRIORITY

Mail Stop PATENT APPLICATION
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

Applicants claim foreign priority benefits under 35 U.S.C. § 119 on the basis of the foreign application identified below:

Japanese Patent Application No. 2003-367272, filed October 28, 2003.

A certified copy of the priority document is enclosed.

Respectfully submitted,

GREER, BURNS & CRAIN, LTD.

By
James K. Folker
Registration No. 37,538

Customer No. 24978

March 30, 2004
300 South Wacker Drive - Suite 2500
Chicago, Illinois 60606
Phone: (312) 360-0080
Fax: (312) 360-9315
P:\DOCS\1924\70199\487502.DOC

PFJA-04008-US

1924.70199
(312) 360-0080

日本国特許庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: ２００３年１０月２８日

出願番号
Application Number: 特願２００３－３６７２７２

[ST. 10/C]: [ＪＰ２００３－３６７２７２]

出願人
Applicant(s): 富士通株式会社

２００４年　２月１８日

特許庁長官
Commissioner,
Japan Patent Office 今井康夫

出証番号　出証特２００４－３０１０６４５

【書類名】　特許願
【整理番号】　0352422
【提出日】　平成15年10月28日
【あて先】　特許庁長官殿
【国際特許分類】　G06F 11/30
【発明者】
　【住所又は居所】　神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内
　【氏名】　面　和成
【発明者】
　【住所又は居所】　神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内
　【氏名】　鳥居　悟
【特許出願人】
　【識別番号】　000005223
　【氏名又は名称】　富士通株式会社
【代理人】
　【識別番号】　100089118
　【弁理士】
　【氏名又は名称】　酒井　宏明
【手数料の表示】
　【予納台帳番号】　036711
　【納付金額】　21,000円
【提出物件の目録】
　【物件名】　特許請求の範囲　1
　【物件名】　明細書　1
　【物件名】　図面　1
　【物件名】　要約書　1
　【包括委任状番号】　9717671

【書類名】特許請求の範囲
【請求項１】
ネットワークに接続された所定のネットワークセグメントに係る通信を監視して該通信がワームによりなされた通信か否かを判定するワーム判定プログラムであって、
情報の取得に係る設定情報に基づいて通信パケットの通信量および該通信パケットの通信アドレスに係る情報を取得する通信情報取得手順と、
前記通信情報取得手順により取得された情報および前記通信がワームによりなされた通信か否かを規定する判定基準に係る情報に基づいて前記通信がワームによりなされた通信か否かを判定するワーム判定手順と、
をコンピュータに実行させることを特徴とするワーム判定プログラム。
【請求項２】
前記ワーム判定手順は、通信を監視する監視対象である前記所定のネットワークセグメントから該所定のネットワークセグメント外部に送信される通信パケットのパケット量が増加し、かつ、該通信パケットの宛先アドレス数が増加した場合に、前記所定のネットワークセグメント内のコンピュータからの通信がワームによりなされた通信であると判定することを特徴とする請求項１に記載のワーム判定プログラム。
【請求項３】
前記ワーム判定手順は、通信を監視する監視対象である前記所定のネットワークセグメント内のコンピュータからの通信がワームによりなされた通信であると以前に判定され、該所定のネットワークセグメントから該所定のネットワークセグメント外部に送信される通信パケットの宛先アドレス数が、前記通信がワームによりなされた通信であると判定する際に前記通信情報取得手段により取得された該所定のネットワークセグメントから該所定のネットワークセグメント外部に送信される通信パケットの宛先アドレス数より増加した場合に、該所定のネットワークセグメント内のコンピュータからの通信が複数のコンピュータに感染したワームによりなされた通信であると判定することを特徴とする請求項２に記載のワーム判定プログラム。
【請求項４】
前記ワーム判定手順は、通信を監視する監視対象である前記所定のネットワークセグメントに対して該所定のネットワークセグメント外部から送信された通信パケットに対する応答通信パケットのパケット量が増加し、かつ、該通信パケットの送信元アドレス数が増加した場合に、前記所定のネットワークセグメント外部のコンピュータからの通信がワームによりなされた通信であると判定することを特徴とする請求項１、２または３に記載のワーム判定プログラム。
【請求項５】
前記ワーム判定手順により前記通信がワームによりなされた通信と判定された場合に、該ワームによりなされる通信を遮断する通信遮断手順を含んだことを特徴とする請求項１～４のいずれか１つに記載のワーム判定プログラム。
【請求項６】
前記通信遮断手順は、ワームにより起動されたプロセスを停止することによりワームによりなされる通信を遮断することを特徴とする請求項５に記載のワーム判定プログラム。
【請求項７】
前記通信遮断手順は、ワームによりなされる通信を該ワームが存在していると判定されるコンピュータのファイアウォール機能を有効にすることにより遮断することを特徴とする請求項５に記載のワーム判定プログラム。
【請求項８】
ネットワークに接続された所定のネットワークセグメントに係る通信を監視して該通信がワームによりなされた通信か否かを判定するワーム判定プログラムを記録したコンピュータ読み取り可能な記録媒体であって、
情報の取得に係る設定情報に基づいて通信パケットの通信量および該通信パケットの通信アドレスに係る情報を取得する通信情報取得手順と、

前記通信情報取得手順により取得された情報および前記通信がワームによりなされた通信か否かを規定する判定基準に係る情報に基づいて前記通信がワームによりなされた通信か否かを判定するワーム判定手順と、

をコンピュータに実行させるワーム判定プログラムを記録したことを特徴とするコンピュータ読み取り可能な記録媒体。

【請求項９】

ネットワークに接続された所定のネットワークセグメントに係る通信を監視して該通信がワームによりなされた通信か否かを判定するワーム判定方法であって、

情報の取得に係る設定情報に基づいて通信パケットの通信量および該通信パケットの通信アドレスに係る情報を取得する通信情報取得工程と、

前記通信情報取得工程により取得された情報および前記通信がワームによりなされた通信か否かを規定する判定基準に係る情報に基づいて前記通信がワームによりなされた通信か否かを判定するワーム判定工程と、

を含んだことを特徴とするワーム判定方法。

【請求項１０】

ネットワークに接続された所定のネットワークセグメントに係る通信を監視して該通信がワームによりなされた通信か否かを判定するワーム判定装置であって、

情報の取得に係る設定情報に基づいて通信パケットの通信量および該通信パケットの通信アドレスに係る情報を取得する通信情報取得手段と、

前記通信情報取得手段により取得された情報および前記通信がワームによりなされた通信か否かを規定する判定基準に係る情報に基づいて前記通信がワームによりなされた通信か否かを判定するワーム判定手段と、

を備えたことを特徴とするワーム判定装置。

【書類名】明細書
【発明の名称】ワーム判定プログラム、ワーム判定プログラムを記憶したコンピュータ読み取り可能な記憶媒体、ワーム判定方法およびワーム判定装置
【技術分野】
【０００１】
この発明は、ネットワークに接続された所定のネットワークセグメントに係る通信を監視して該通信がワームによりなされた通信か否かを判定するワーム判定プログラム、ワーム判定プログラムを記憶したコンピュータ読み取り可能な記憶媒体、ワーム判定方法およびワーム判定装置に関し、特に、サーバ装置かクライアント装置かに拘らず通信がワームによりなされたものか否かを容易にかつ効率的に判定することができるワーム判定プログラム、ワーム判定プログラムを記憶したコンピュータ読み取り可能な記憶媒体、ワーム判定方法およびワーム判定装置に関するものである。
【背景技術】
【０００２】
近年、自己増殖を繰り返しながらコンピュータに次々と感染し、コンピュータに悪影響を及ぼすワームと呼ばれるコンピュータウィルスによる被害が拡大してきている。古くは、ワームは、フレキシブルディスク（ＦＤ）やＣＤ－ＲＯＭなどを介してコンピュータに感染していたため感染力がそれほど大きくはなかったが、最近は、インターネットが普及するにつれワームの感染力が加速度的に大きくなり、ワームに対する防御をいかにおこなうかが大きな問題となっている。
【０００３】
そのため、特許文献１には、ワームを含んでいるかどうかを検査する検査対象を仮想的に構築したコンピュータ環境に導入し、その検査対象が仮想的なコンピュータ環境における所定のファイルを変更するか否かを監視することにより、ワームであるか否かを判定するワームの検査方法が開示されている。
【０００４】
また、非特許文献１には、ワームにより攻撃された場合に必ず生じるサーバ装置の振る舞い（データＩ／Ｏやシステムコールなどの系列）をあらかじめ監視ルールとして定義しておき、ワームを含んでいるかどうかを検査する検査対象をアクセス検査サーバ装置に導入して、その動作を監視することによりワームによる攻撃を検出するＷｅｂサーバ防御システムが開示されている。
【０００５】
【特許文献１】特開２００２－３４２１０６号公報
【非特許文献１】日本電気株式会社、”プレスリリース”、［ｏｎｌｉｎｅ］、２００３年４月１１日、［平成１５年１０月２８日検索］、インターネット＜ＵＲＬ：ｈｔｔｐ：／／ｗｗｗ．ｎｅｃ．ｃｏ．ｊｐ／ｐｒｅｓｓ／ｊａ／０３０４／１１０１．ｈｔｍｌ＞
【発明の開示】
【発明が解決しようとする課題】
【０００６】
しかしながら、上記特許文献１の従来技術では、通信をおこなう度に検査対象をあらかじめ構築しておいた仮想的なコンピュータ環境に導入し、その仮想的なコンピュータ環境に対する感染の有無を検査する必要があるため、すべての通信に関してワームの検出をおこなうのは効率的でなく、ワームを含んでいる危険性のある通信のみに対して検査をおこなうにしても、その危険性を判定する基準を定めることが難しいという問題があった。
【０００７】
また、非特許文献２の従来技術では、ワームにより攻撃された場合に必ず生じるサーバ装置の振る舞いを監視ルールとして定義しておくこととしているが、多くの用途に使用され、さまざまな振る舞いを示すクライアント装置に対して、ワーム攻撃による振る舞いと通常使用による振る舞いとを区別する監視ルールを定義することが難しいという問題があ

った。

【０００８】

この発明は、上述した従来技術による問題点を解消するためになされたものであり、サーバ装置かクライアント装置かに拘らず通信がワームによりなされたものか否かを容易にかつ効率的に判定することができるワーム判定プログラム、ワーム判定プログラムを記憶したコンピュータ読み取り可能な記憶媒体、ワーム判定方法およびワーム判定装置を提供することを目的とする。

【課題を解決するための手段】

【０００９】

上述した課題を解決し、目的を達成するため、本発明は、ネットワークに接続された所定のネットワークセグメントに係る通信を監視して該通信がワームによりなされた通信か否かを判定するワーム判定プログラムであって、情報の取得に係る設定情報に基づいて通信パケットの通信量および該通信パケットの通信アドレスに係る情報を取得する通信情報取得手順と、前記通信情報取得手順により取得された情報および前記通信がワームによりなされた通信か否かを規定する判定基準に係る情報に基づいて前記通信がワームによりなされた通信か否かを判定するワーム判定手順と、をコンピュータに実行させることを特徴とする。

【００１０】

また、本発明は、前記ワーム判定手順により前記通信がワームによりなされた通信と判定された場合に、前記情報の取得に係る設定情報を変更する設定情報変更手順をさらに含み、前記通信情報取得手順は、前記情報取得設定変更手順により変更された情報の取得に係る設定情報に基づいて通信パケットの通信量および該通信パケットの通信アドレスに係る情報を取得することを特徴とする。

【００１１】

また、本発明は、前記ワーム判定手順により前記通信がワームによりなされた通信と判定された場合に、前記判定基準に係る情報を変更する判定基準情報変更手順をさらに含み、前記ワーム判定手順は、前記通信情報取得手順により取得された情報および前記判定基準情報変更手順により変更された判定基準に係る情報に基づいて前記通信がワームによりなされた通信か否かを判定することを特徴とする。

【００１２】

また、本発明は、前記ワーム判定手順は、通信を監視する監視対象である前記所定のネットワークセグメントから該所定のネットワークセグメント外部に送信される通信パケットのパケット量が増加し、かつ、該通信パケットの宛先アドレス数が増加した場合に、前記所定のネットワークセグメント内のコンピュータからの通信がワームによりなされた通信であると判定することを特徴とする。

【００１３】

また、本発明は、前記ワーム判定手順は、通信を監視する監視対象である前記所定のネットワークセグメント内のコンピュータからの通信がワームによりなされた通信であると以前に判定され、該所定のネットワークセグメントから該所定のネットワークセグメント外部に送信される通信パケットの宛先アドレス数が、前記通信がワームによりなされた通信であると判定する際に前記通信情報取得手段により取得された該所定のネットワークセグメントから該所定のネットワークセグメント外部に送信される通信パケットの宛先アドレス数より増加した場合に、該所定のネットワークセグメント内のコンピュータからの通信が複数のコンピュータに感染したワームによりなされた通信であると判定することを特徴とする。

【００１４】

また、本発明は、前記ワーム判定手順は、通信を監視する監視対象である前記所定のネットワークセグメントに対して該所定のネットワークセグメント外部から送信された通信パケットに対する応答通信パケットのパケット量が増加し、かつ、該通信パケットの送信元アドレス数が増加した場合に、前記所定のネットワークセグメント外部のコンピュータ

からの通信がワームによりなされた通信であると判定することを特徴とする。

【００１５】

また、本発明は、前記ワーム判定手順は、前記通信をワームによりなされた通信と判定した場合に、該通信をおこなったコンピュータもしくは通信状況に係る情報をさらに出力することを特徴とする。

【００１６】

また、本発明は、前記ワーム判定手順は、前記通信をワームによりなされた通信と判定した場合に、ワームによりなされる通信に係るあらかじめ登録された特徴とワームによりなされたと判定した通信に係る特徴とを比較することにより前記ワームの種類を推定することを特徴とする。

【００１７】

また、本発明は、前記ワーム判定手順により前記通信がワームによりなされた通信と判定された場合に、該ワームによりなされる通信を遮断する通信遮断手順を含んだことを特徴とする。

【００１８】

また、本発明は、前記通信遮断手順は、ワームにより起動されたプロセスを停止することによりワームによりなされる通信を遮断することを特徴とする。

【００１９】

また、本発明は、前記通信遮断手順は、ワームによりなされる通信を該ワームが存在していると判定されるコンピュータのファイアウォール機能を有効にすることにより遮断することを特徴とする。

【００２０】

また、本発明は、ネットワークに接続された所定のネットワークセグメントに係る通信を監視して該通信がワームによりなされた通信か否かを判定するワーム判定プログラムを記録したコンピュータ読み取り可能な記録媒体であって、情報の取得に係る設定情報に基づいて通信パケットの通信量および該通信パケットの通信アドレスに係る情報を取得する通信情報取得手順と、前記通信情報取得手順により取得された情報および前記通信がワームによりなされた通信か否かを規定する判定基準に係る情報に基づいて前記通信がワームによりなされた通信か否かを判定するワーム判定手順と、をコンピュータに実行させるワーム判定プログラムを記録したことを特徴とする。

【００２１】

また、本発明は、ネットワークに接続された所定のネットワークセグメントに係る通信を監視して該通信がワームによりなされた通信か否かを判定するワーム判定方法であって、情報の取得に係る設定情報に基づいて通信パケットの通信量および該通信パケットの通信アドレスに係る情報を取得する通信情報取得工程と、前記通信情報取得工程により取得された情報および前記通信がワームによりなされた通信か否かを規定する判定基準に係る情報に基づいて前記通信がワームによりなされた通信か否かを判定するワーム判定工程と、を含んだことを特徴とする。

【００２２】

また、本発明は、ネットワークに接続された所定のネットワークセグメントに係る通信を監視して該通信がワームによりなされた通信か否かを判定するワーム判定装置であって、情報の取得に係る設定情報に基づいて通信パケットの通信量および該通信パケットの通信アドレスに係る情報を取得する通信情報取得手段と、前記通信情報取得手段により取得された情報および前記通信がワームによりなされた通信か否かを規定する判定基準に係る情報に基づいて前記通信がワームによりなされた通信か否かを判定するワーム判定手段と、を備えたことを特徴とする。

【発明の効果】

【００２３】

本発明によれば、情報の取得に係る設定情報に基づいて通信パケットの通信量および通信パケットの通信アドレスに係る情報を取得し、取得された情報および通信がワームによ

りなされた通信か否かを規定する判定基準に係る情報に基づいて通信がワームによりなされた通信か否かを判定することとしたので、サーバ装置かクライアント装置かに拘らず通信がワームによりなされたものか否かを容易にかつ効率的に判定することができるという効果を奏する。

【００２４】

また、本発明によれば、通信がワームによりなされた通信と判定された場合に、情報の取得に係る設定情報を変更し、変更された情報の取得に係る設定情報に基づいて通信パケットの通信量および通信パケットの通信アドレスに係る情報を取得することとしたので、通信がワームによりなされた通信と判定された場合に情報の取得に係る設定情報を変更することにより、さらに詳細にワームの挙動を監視することができるという効果を奏する。

【００２５】

また、本発明によれば、通信がワームによりなされた通信と判定された場合に、判定基準に係る情報を変更し、取得された情報および変更された判定基準に係る情報に基づいて通信がワームによりなされた通信か否かを判定することとしたので、通信がワームによりなされた通信と判定された場合に判定基準に係る情報を変更することにより、さらに厳密に通信がワームによりなされた通信か否かを判定することができるという効果を奏する。

【００２６】

また、本発明によれば、通信を監視する監視対象である所定のネットワークセグメントからその所定のネットワークセグメント外部に送信される通信パケットのパケット量が増加し、かつ、通信パケットの宛先アドレス数が増加した場合に、所定のネットワークセグメント内のコンピュータからの通信がワームによりなされた通信であると判定することとしたので、ワームによる通信が所定のネットワークセグメント内のコンピュータからなされた場合に、それを容易にかつ効率的に判定することができるという効果を奏する。

【００２７】

また、本発明によれば、通信を監視する監視対象である所定のネットワークセグメント内のコンピュータからの通信がワームによりなされた通信であると以前に判定され、所定のネットワークセグメントからその所定のネットワークセグメント外部に送信される通信パケットの宛先アドレス数が、通信がワームによりなされた通信であると判定する際に取得された所定のネットワークセグメントからその所定のネットワークセグメント外部に送信される通信パケットの宛先アドレス数より増加した場合に、所定のネットワークセグメント内のコンピュータからの通信が複数のコンピュータに感染したワームによりなされた通信であると判定することとしたので、ワームによる通信が所定のネットワークセグメント内の複数のコンピュータからなされた場合に、それを容易にかつ効率的に判定することができるという効果を奏する。

【００２８】

また、本発明によれば、通信を監視する監視対象である所定のネットワークセグメントに対してその所定のネットワークセグメント外部から送信された通信パケットに対する応答通信パケットのパケット量が増加し、かつ、通信パケットの送信元アドレス数が増加した場合に、所定のネットワークセグメント外部のコンピュータからの通信がワームによりなされた通信であると判定することとしたので、ワームによる通信が所定のネットワークセグメント外のコンピュータからなされた場合に、それを容易にかつ効率的に判定することができるという効果を奏する。

【００２９】

また、本発明によれば、通信をワームによりなされた通信と判定した場合に、通信をおこなったコンピュータもしくは通信状況に係る情報をさらに出力することとしたので、出力されたコンピュータに係る情報を基にしてワームに感染している可能性のあるコンピュータを特定することができるという効果を奏する。

【００３０】

また、本発明によれば、通信をワームによりなされた通信と判定した場合に、ワームによりなされる通信に係るあらかじめ登録された特徴とワームによりなされたと判定した通

信に係る特徴とを比較することによりワームの種類を推定することとしたので、推定されたワームの種類の情報を基にしてワームの攻撃に適切に対応することができるという効果を奏する。

【００３１】

また、本発明によれば、通信がワームによりなされた通信と判定された場合に、ワームによりなされる通信を遮断することとしたので、ワームの増殖を効果的に抑制することができるという効果を奏する。

【００３２】

また、本発明によれば、ワームにより起動されたプロセスを停止することによりワームによりなされる通信を遮断することとしたので、ワームがおこなう処理自体を停止させることにより、ワームの増殖を効果的に抑制することができるという効果を奏する。

【００３３】

また、本発明によれば、ワームによりなされる通信をワームが存在していると判定されるコンピュータのファイアウォール機能を有効にすることにより遮断することとしたので、ワームによりなされる通信をワームに感染しているコンピュータに遮断させることにより、ワームの増殖を効果的に抑制することができるという効果を奏する。

【発明を実施するための最良の形態】

【００３４】

以下に添付図面を参照して、この発明に係るワーム判定プログラム、ワーム判定プログラムを記憶したコンピュータ読み取り可能な記憶媒体、ワーム判定方法およびワーム判定装置の好適な実施の形態を詳細に説明する。

【実施例】

【００３５】

まず、本実施例に係るネットワークセグメントの概念について説明する。図１６は、本実施例に係るネットワークセグメントの概念を説明する概念図である。図１６に示すように、本実施例におけるネットワークセグメントは、複数の階層からなる構造を有している。

【００３６】

たとえば、最も小規模なネットワークセグメント１６ａは、ワーム判定プログラムが導入されたコンピュータを１台だけ含むものである。この場合、そのコンピュータがネットワークセグメント１６ａに係る通信を監視してワーム判定処理をおこなう。それよりもやや大きい規模のネットワークセグメント１６ｂは、部署のイントラネット単位で構成されるセグメントであり、そのネットワークセグメント１６ｂに対してワーム判定装置１７ａが接続され、そのワーム判定装置１７ａが、ワークセグメント１６ｂに係る通信を監視してワーム判定処理をおこなう。

【００３７】

さらに大きい規模であるネットワークセグメント１６ｃは、企業のイントラネット単位で構成されるセグメントであり、そのネットワークセグメント１６ｃに対してワーム判定装置１７ｂが接続され、そのワーム判定装置１７ｂが、ワークセグメント１６ｃに係る通信を監視してワーム判定処理をおこなう。そして、より大規模のネットワークセグメント１６ｄは、ＩＳＰ（Ｉｎｔｅｒｎｅｔ　Ｓｅｒｖｉｃｅ　Ｐｒｏｖｉｄｅｒ）単位で構成されるセグメントであり、そのネットワークセグメント１６ｄに対してワーム判定装置１７ｃが接続され、そのワーム判定装置１７ｃが、ワークセグメント１６ｄに係る通信を監視してワーム判定処理をおこなう。

【００３８】

このように、ネットワークセグメントの規模および形態には様々なものが考えられ、そのさまざまな規模および形態のネットワークセグメントに対して、本発明に係るワーム判定システムの適用をおこなうことができる。

【００３９】

つぎに、本実施例に係るワーム判定システムの概念について説明する。図１は、本実施

例に係るワーム判定システムの概念について説明する概念図である。図１に示すように、このワーム判定システムは、サーバ装置やクライアント装置などを少なくとも１台以上含むネットワークセグメント１０ａ～１０ｄが、ワーム判定装置２０ａ～２０ｄを介してネットワーク１１に接続された構成となっている。ここで、ネットワーク１１とは、インターネット、イントラネット、ＩＳＰのネットワークなどを指している。

【００４０】

このワーム判定装置２０ａ～２０ｄは、各ネットワークセグメント１０ａ～１０ｄに他のネットワークセグメント１０ａ～１０ｄから送信される通信パケットと、各ネットワークセグメント１０ａ～１０ｄが他のネットワークセグメント１０ａ～１０ｄに送信する通信パケットとを監視して、その通信パケットによる通信がワームによりなされた通信であるか否かを判定する処理をおこなう。

【００４１】

具体的には、通信パケットの単位時間当たりのパケット数、各通信パケットの送信元ＩＰアドレスおよび宛先ＩＰアドレスの情報などを取得し、取得した情報に基づいて監視対象としているネットワークセグメント１０ａ～１０ｄ外からのワームの攻撃があるか否かや、そのネットワークセグメント１０ａ～１０ｄ内から他のネットワークセグメント１０ａ～１０ｄ内のコンピュータに対してワームの攻撃がなされているか否か等を判定する。

【００４２】

ここで、ワームに感染した場合に生じる通信パケットの単位時間当たりのパケット数、各通信パケットの送信元ＩＰアドレスおよび宛先ＩＰアドレスの情報の変化は、サーバ装置やクライアント装置などのコンピュータの種類に依らず顕著に現れるため、このワーム判定システムにおいては、サーバ装置かクライアント装置かに拘らず容易にかつ効率的にワームを検出することができる。

【００４３】

また、ワームの特徴をあらかじめ登録しておき、その特徴を参照してワームによる通信を検出するのではなく、通信パケットの単位時間当たりのパケット数、各通信パケットの送信元ＩＰアドレスおよび宛先ＩＰアドレスの情報の変化を基にしてワームによる通信か否かを判定するので、未知のワームに対しても適切に対処することができる。

【００４４】

つぎに、本実施例に係るワーム判定装置２０ａ～２０ｄの機能的構成について説明する。図２は、本実施例に係るワーム判定装置２０ａ～２０ｄの機能的構成について説明する機能ブロック図である。各ワーム判定装置２０ａ～２０ｄは、同様の機能を有するので、ここでは、ワーム判定装置２０ａの機能的構成について説明する。

【００４５】

図２に示すように、このワーム判定装置２０ａは、ネットワークセグメントＡ１０ａおよびネットワークセグメントＡ１０ａを除いたネットワーク１２にＬＡＮ２１およびネットワーク２１を介して接続されている。ここで、ＬＡＮ２１は、イントラネットなどのネットワークである。

【００４６】

ワーム判定装置２０ａは、本発明に係る装置であり、情報の取得に係る設定情報に基づいて通信パケットの通信量および通信パケットの通信アドレスに係る情報を取得し、取得した情報と、通信がワームによりなされた通信か否かを規定する判定基準に係る情報とに基づいて通信がワームによりなされた通信か否かを判定する判定装置である。

【００４７】

このワーム判定装置２０ａは、インターフェース部２００、入力部２１０、表示部２２０、記憶部２３０および制御部２４０を有する。インターフェース部２００は、ネットワークセグメントＡ１０ａとネットワークセグメントＡを除くネットワーク１２との間の通信データの授受を、ＬＡＮ２１およびネットワーク２１を介して中継するネットワークインターフェースである。

【００４８】

入力部２１０は、キーボードやマウスなどの入力デバイスであり、表示部２２０は、ディスプレイなどの表示デバイスである。記憶部２３０は、ハードディスク装置などの記憶デバイスであり、この記憶部２３０には、設定データ２３０ａ、通信ログデータ２３０ｂおよびワームデータ２３０ｃが記憶されている。

【００４９】

設定データ２３０ａは、通信パケットの通信量および通信パケットの通信アドレスに係る情報の取得に係る設定情報や、監視している通信がワームによりなされた通信か否かを規定する判定基準に係る情報など、さまざまな設定情報を記憶したデータである。

【００５０】

図３は、図２に示した設定データ２３０ａの一例を示す図である。この設定データ２３０ａは、設定項目、初期設定およびＳＹＮパケット異常検知後の設定の各項目を有する。設定項目は、設定データ２３０ａにおいて設定される各項目であり、初期設定は、通常監視時に参照される設定情報であり、ＳＹＮパケット異常検知後の設定は、監視していたＳＹＮパケットに異常が検知された場合に、初期設定の代わりに参照される設定情報である。このＳＹＮパケットの異常は、後に説明するように、単位時間内に計測したＳＹＮパケットの数が所定の閾値以上で、宛先ＩＰアドレス数が所定の閾値以上となった場合を意味している。

【００５１】

上記設定項目には、具体的には、ＳＹＮパケットの計測単位時間、ＳＹＮ　ＡＣＫパケットの計測単位時間、ＵＤＰパケットの計測単位時間、ＩＣＭＰ（ｒｅｑｕｅｓｔ）パケットの計測単位時間、ＩＣＭＰ（ｒｅｐｌｙ）パケットの計測単位時間、宛先ＩＰアドレスの計測単位時間、送信元ＩＰアドレスの計測単位時間、宛先ポート番号の参照、ＳＹＮパケット数の閾値、ＳＹＮ　ＡＣＫパケット数の閾値、ＵＤＰパケットの閾値、ＩＣＭＰ（ｒｅｑｕｅｓｔ）パケットの閾値、ＩＣＭＰ（ｒｅｐｌｙ）パケットの閾値、宛先ＩＰアドレス数の閾値、送信元ＩＰアドレス数の閾値、監視場所、監視するネットワークの方向、遮断および検知から遮断までの時間が登録されている。

【００５２】

ＳＹＮパケットの計測単位時間、ＳＹＮ　ＡＣＫパケットの計測単位時間、ＵＤＰパケットの計測単位時間、ＩＣＭＰ（ｒｅｑｕｅｓｔ）パケットの計測単位時間およびＩＣＭＰ（ｒｅｐｌｙ）パケットの計測単位時間は、それぞれ、ＴＣＰ（Ｔｒａｎｓｍｉｓｓｉｏｎ　Ｃｏｎｔｒｏｌ　Ｐｒｏｔｏｃｏｌ）ベースのパケットであるＳＹＮパケット、ＳＹＮパケットをコンピュータが受信した際の応答として送信されるＳＹＮ　ＡＣＫパケット、ＵＤＰ（Ｕｓｅｒ　Ｄａｔａｇｒａｍ　Ｐｒｏｔｏｃｏｌ）ベースのパケットであるＵＤＰパケット、相手コンピュータの動作確認メッセージを送信するＩＣＭＰ（Ｉｎｔｅｒｎｅｔ　Ｃｏｎｔｒｏｌ　Ｍｅｓｓａｇｅ　Ｐｒｏｔｏｃｏｌ）（ｒｅｑｕｅｓｔ）パケット、そのＩＣＰＭ（ｒｅｑｕｅｓｔ）パケットの応答として送信されるＩＣＭＰ（ｒｅｐｌｙ）パケットの数を計測する単位時間である。たとえば、この単位時間が１ｓｅｃであるということは、１秒間の上記パケットの送信数または受信数を１秒ごとに計測することを意味する。

【００５３】

また、宛先ＩＰアドレスの計測単位時間および送信元ＩＰアドレスの計測単位時間は、上記各パケットの宛先ＩＰアドレスおよび送信元ＩＰアドレスを計測する単位時間である。たとえば、この単位時間が１ｓｅｃであるということは、１秒間の上記パケットの宛先ＩＰアドレスおよび送信元ＩＰアドレスを１秒ごとに計測することを意味する。宛先ポート番号の参照は、上記各パケットの宛先ポート番号をリアルタイムで参照するか否かを設定する項目であり、「ＯＮ」または「ＯＦＦ」のいずれかに設定される。

【００５４】

ＳＹＮパケット数の閾値、ＳＹＮ　ＡＣＫパケット数の閾値、ＵＤＰパケットの閾値、ＩＣＭＰ（ｒｅｑｕｅｓｔ）パケットの閾値、ＩＣＭＰ（ｒｅｐｌｙ）パケットの閾値は、ワームによりなされた通信がおこなわれているか否かを判定する際に使用されるパケッ

ト数の閾値情報である。宛先ＩＰアドレス数の閾値および送信元ＩＰアドレス数の閾値は、ワームによりなされた通信がおこなわれているか否かを判定する際に使用される宛先ＩＰアドレス数および送信元ＩＰアドレス数の閾値情報である。ここで、宛先ＩＰアドレス数または送信元ＩＰアドレス数は、宛先ＩＰアドレスの計測単位時間または送信元ＩＰアドレスの計測単位時間内に計測された異なる宛先ＩＰアドレスまたは送信元ＩＰアドレスの数である。

【００５５】

監視場所は、パケットを監視するネットワークドライバを設定する項目であり、たとえば、ネットワークドライバ「Ｅｔｈ０」などと設定する。監視するネットワークの方向は、監視するパケット通信の方向を設定する項目である。たとえば、ワーム判定装置２０ａが接続されているネットワークセグメントＡ１０ａから外に送信されるパケットのみを監視する場合には、「Ｏｕｔｇｏｉｎｇ」に設定され、ネットワークセグメントＡを除くネットワーク１２からネットワークセグメントＡ１０ａに対して送信されるパケットを監視する場合には、「ｉｎｃｏｍｉｎｇ」に設定され、それら両方のパケットを監視する場合には、「ｂｏｔｈ」に設定される。

【００５６】

遮断は、パケット通信がワームによりなされた通信と判定された場合に、通信の遮断をおこなうか否かを設定する項目であり、「ＯＮ」または「ＯＦＦ」のいずれかに設定される。検知から遮断までの時間は、ワームによりなされたパケット通信を検知した場合に、パケット通信を遮断するまでの待ち時間を設定する項目であり、たとえば、「５ｓｅｃ」などと設定される。

【００５７】

図２の説明に戻ると、通信ログデータ２３０ｂは、パケット通信の通信記録を記憶したデータである。具体的には、図３で示した設定データ２３０ａに基づいて取得された通信パケットのパケット数やＩＰアドレス数の情報、ワームによりなされた通信か否かを判定した判定結果の情報などを記憶している。

【００５８】

図４は、図２に示した通信ログデータ２３０ｂの一例を示す図である。図４に示すように、この通信ログデータ２３０ｂは、計測時間、パケット数およびＩＰアドレス数の各項目を有する。計測時間は、計測をおこなった時間であり、パケット数は、各計測時間において計測されたパケット数である。このパケット数は、さらに、ＳＹＮパケット数、ＳＹＮ　ＡＣＫパケット数、ＵＤＰパケット数、ＩＣＭＰ（ｒｅｑｕｅｓｔ）パケット数およびＩＣＭＰ（ｒｅｐｌｙ）パケット数の項目を有し、各パケットの種類ごとに計測されたパケット数が記憶される。

【００５９】

ＩＰアドレス数は、各計測時間において計測されたＩＰアドレス数である。このＩＰアドレス数は、さらに、宛先ＩＰアドレス数および送信元ＩＰアドレス数の項目を有し、各計測時間における通信パケットの宛先ＩＰアドレス数および送信元ＩＰアドレス数の情報が記憶される。

【００６０】

また、図３に示した設定データ２３０ａの「宛先ポート番号の参照」の項目が「ＯＮ」である場合には、通信ログデータ２３０ｂに、通信情報取得部２４０ａにより取得された最頻出宛先ポート番号の情報が各計測時間ごとに記憶される（図４には、図示せず。）。さらに、この通信ログデータ２３０ｂには、ワームによる通信がおこなわれたと判定された場合に、ワームの通信方法や通信速度、通信特徴が類似しているワームの情報などとともにその判定結果が記憶される（図４には、図示せず。）。

【００６１】

図２の説明に戻ると、ワームデータ２３０ｃは、ワームによりなされる通信の特徴を記憶したデータである。具体的には、このワームデータ２３０ｃは、過去に発見されたワームが単位時間内に他のコンピュータのスキャンをおこなうスキャン速度の情報や、攻撃す

る宛先ポート番号などのワームの特徴情報を記憶する。

【００６２】

制御部２４０は、ワーム判定装置２０ａを全体制御する制御部である。この制御部２４０は、通信情報取得部２４０ａ、ワーム判定部２４０ｂ、設定データ変更部２４０ｃおよび通信遮断部２４０ｄを有する。

【００６３】

通信情報取得部２４０ａは、記憶部２３０に記憶された設定データ２３０ａに基づいて、通信パケットの通信量および通信パケットの通信アドレスに係る情報を取得する取得部である。具体的には、この通信情報取得部２４０ａは、通信パケットのパケット数を計測するとともに、通信パケットのヘッダから宛先ＩＰアドレスや送信元ＩＰアドレスの情報を取得し、宛先ＩＰアドレス数や送信元ＩＰアドレス数を計測したり、通信パケットの宛先ポート番号などの情報から最頻出宛先ポート番号の情報を取得したりして、通信ログデータ２３０ｂに記憶する処理などをおこなう。

【００６４】

ワーム判定部２４０ｂは、通信情報取得部２４０ａにより取得された情報、および、記憶部２３０に記憶された設定データ２３０ａに基づいて、監視対象としているパケット通信がワームによりなされた通信か否かを判定する判定部である。つぎに、この判定処理の内容を具体的に説明する。

【００６５】

図５は、図２に示したワーム判定部２４０ｂがおこなうパケットの種類ごとのワーム判定処理の例を示す図である。図５では、ワーム判定部２４０ｂがおこなう判定処理の内容を３つのケースに分けて示している。ケース１は、Ｏｕｔｇｏｉｎｇ通信を監視している際に、ＳＹＮパケット数が増加し、かつ、宛先ＩＰアドレス数が増加したという状況が観測された場合である。

【００６６】

この状況は、ネットワークセグメントＡ１０ａ外のさまざまなコンピュータにＳＹＮパケットが多数送信されていることを意味するので、ワーム判定部２４０ｂは、ＴＣＰベースのワームがネットワークセグメントＡ１０ａ内のコンピュータに感染しており、ネットワークセグメントＡ１０ａ外のコンピュータに対してランダムスキャンをおこなっていると判定する。この場合、ワーム判定部２４０ｂは、さらに宛先ポート番号を計測し、最頻出宛先ポート番号からどのサービスを狙ったワームかを検出する。たとえば、計測された最頻出宛先ポート番号が８０番であれば、Ｗｅｂサービスを狙ったワームであると判定できる。

【００６７】

ケース２は、Ｏｕｔｇｏｉｎｇ通信を監視している際に、ＵＤＰパケット数が増加し、かつ、宛先ＩＰアドレス数が増加したという状況が観測された場合である。この状況は、ネットワークセグメントＡ１０ａ外のさまざまなコンピュータにＵＤＰパケットが多数送信されていることを意味するので、ワーム判定部２４０ｂは、ＵＤＰベースのワームがネットワークセグメントＡ１０ａ内のコンピュータに感染しており、ネットワークセグメントＡ１０ａ外のコンピュータに対してランダムスキャンをおこなっていると判定する。この場合、ワーム判定部２４０ｂは、さらに宛先ポート番号を計測し、最頻出宛先ポート番号からどのサービスを狙ったワームかを検出する。たとえば、計測された最頻出宛先ポート番号が５３番であれば、ＤＮＳサービスを狙ったワームであると判定できる。

【００６８】

ケース３は、Ｏｕｔｇｏｉｎｇ通信を監視している際に、ＩＣＭＰ（ｒｅｑｕｅｓｔ）パケット数が増加し、かつ、宛先ＩＰアドレス数が増加したという状況が観測された場合である。この状況は、ネットワークセグメントＡ１０ａ外のさまざまなコンピュータにＩＣＭＰ（ｒｅｑｕｅｓｔ）パケットが多数送信されていることを意味する。この場合、ワーム判定部２４０ｂは、パケットの送信がワームによるものか否かの判定を一時保留する。これは、ＩＣＭＰ（ｒｅｑｕｅｓｔ）パケットは、相手コンピュータの動作確認メッセ

ージを送信するパケットであり、ＩＣＭＰ（ｒｅｑｕｅｓｔ）パケットのパケット数および宛先ＩＰアドレス数が増加しただけでは、ワームによるランダムスキャンがおこなわれているのかどうかが不明なためである。

【００６９】

この場合、ワーム判定部２４０ｂは、その後送信されるＳＹＮパケットあるいはＵＤＰパケットを監視して、ケース１または２のように状況を判定することによりＴＣＰベースのワームか、あるいはＵＤＰベースのワームかを判定し、さらに宛先ポート番号を計測して、その最頻出宛先ポート番号からどのサービスを狙ったワームかを検出する処理をおこなう。ここでは、ケース１～３の３つの場合について説明したが、さらにさまざまな状況を追加することにより、各パケットの種類に対してワームによる通信か否かを詳細に判定することができる。

【００７０】

図６は、図２に示したワーム判定部２４０ｂがおこなうネットワークセグメント外からのワームスキャンの有無を判定する処理の一例を示す図である。ここでは、ＳＹＮ　ＡＣＫパケットに異常が検出された場合を示している。図６に示すように、ワーム判定部２４０ｂは、通信ログデータ２３０ｂを参照し、各パケットのパケット数およびＩＰアドレス数が設定データ２３０ａに記憶されている閾値以上であるか否かを調べる。たとえば、ワーム判定部２４０ｂは、ＳＹＮ　ＡＣＫパケット数の閾値が「１０」、送信元ＩＰアドレス数の閾値が「１０」である場合には、計測時間「１０：００：３５～１０：００：３６」においてＳＹＮ　ＡＣＫパケット数「３０」が閾値「１０」以上であり、かつ、送信元ＩＰアドレス数「３６」が閾値「１０」以上であるので、ＳＹＮ　ＡＣＫパケットの異常を検出する。

【００７１】

また、ワーム判定部２４０ｂは、通信情報取得部２４０ａにより取得されたＳＹＮ　ＡＣＫパケットの最頻出宛先ポート番号の情報から、どのサービスを狙ったワームかを検出する処理をおこなう。図６の通信ログデータ２３０ｂには、取得された最頻出宛先ポート番号「８０」の情報が示されている。最頻出宛先ポート番号の欄に示されている百分率の情報（「９０％」および「９２％」）は、計測時間内に「ＳＹＮ　ＡＣＫパケット数」および「送信元ＩＰアドレス数」の監視をおこなった全パケットのうち、最頻出宛先ポート番号が「８０」番であったパケットの割合を示したものである。

【００７２】

その後、ワーム判定部２４０ｂは、上記情報を基にしてワームスキャンの有無を判定し、ワーム判定結果６０を出力する処理をおこなう。具体的には、ワーム判定部２４０ｂは、ＳＹＮパケットを受信した際の応答であるＳＹＮ　ＡＣＫパケットがネットワークセグメントＡ１０ａ内から閾値より多く送信され、かつ、ＳＹＮ　ＡＣＫパケットの送信元ＩＰアドレス数が閾値より多いため、ネットワークセグメントＡを除くネットワーク１２のコンピュータからネットワークセグメントＡ１０ａ内のコンピュータに対してワームによるランダムスキャンがなされていると判定し、そのワーム判定結果６０を出力する。

【００７３】

このワーム判定結果６０は、スキャン方法、スキャン元ＩＰアドレス、最頻出宛先ポート番号および警告メッセージの情報を含んでいる。スキャン方法は、ワームがランダムスキャンをおこなう際に使用するパケットの種類を示しており、スキャン元ＩＰアドレスは、ランダムスキャンに使用されているパケットを送信しているコンピュータのＩＰアドレスである。このスキャン元ＩＰアドレスの情報は、パケットのヘッダより取得することができる。最頻出宛先ポート番号は、通信ログデータ２３０ｂに含まれる最頻出宛先ポート番号であり、警告メッセージは、ユーザに判定結果を通知して注意を促すメッセージである。図６の例では、ネットワークセグメントＡを除くネットワーク１２のコンピュータからのランダムスキャンが検出されたので、Ｗｅｂサービスの脆弱性を狙うワームが外部から進入する可能性があることをユーザに通知する。

【００７４】

図７は、図２に示したワーム判定部２４０ｂがおこなうワーム感染の有無を判定する処理の一例を示す図である。ここでは、ＳＹＮパケットに異常が検出された場合を示している。図７に示すように、ワーム判定部２４０ｂは、通信ログデータ２３０ｂを参照し、各パケットのパケット数およびＩＰアドレス数が設定データ２３０ａに記憶されている閾値以上であるか否かを調べる。たとえば、ワーム判定部２４０ｂは、ＳＹＮパケット数の閾値が「１０」、宛先ＩＰアドレス数の閾値が「１０」である場合には、計測時間「１０：００：３７～１０：００：３８」においてＳＹＮパケット数「２２」が閾値「１０」以上であり、かつ、宛先ＩＰアドレス数「２８」が閾値「１０」以上であるので、ＳＹＮパケットの異常を検出する。

【００７５】

また、ワーム判定部２４０ｂは、通信情報取得部２４０ａにより取得されたＳＹＮパケットの最頻出宛先ポート番号の情報から、どのサービスを狙ったワームかを検出する処理をおこなう。図７の通信ログデータ２３０ｂには、取得された最頻出宛先ポート番号「８０」の情報と、監視をおこなった全パケットのうち最頻出宛先ポート番号が「８０」番であったパケットの割合の情報（「９４％」および「８９％」）とが、ＳＹＮパケット数および宛先ＩＰアドレス数のそれぞれの計測項目ごとに示されている。

【００７６】

その後、ワーム判定部２４０ｂは、上記情報を基にしてワーム感染の有無を判定し、ワーム判定結果７０を出力する処理をおこなう。具体的には、ワーム判定部２４０ｂは、ＳＹＮパケットが、ネットワークセグメントＡ１０ａ内から閾値より多く送信され、かつ、ＳＹＮパケットの宛先ＩＰアドレス数が閾値より多いため、ネットワークセグメントＡ１０ａ内のコンピュータからネットワークセグメントＡを除くネットワーク１２のコンピュータに対してワームによるランダムスキャンがなされていると判定し、そのワーム判定結果７０を出力する。

【００７７】

このワーム判定結果７０は、スキャン方法、スキャン速度、感染台数、感染コンピュータ名、感染コンピュータＩＰアドレス、最頻出宛先ポート番号および警告メッセージの情報を含んでいる。スキャン方法は、ワームがランダムスキャンをおこなう際に使用するパケットの種類を示しており、スキャン速度は、１秒間にスキャンがなされた速度の情報である。感染台数は、ワームに感染した可能性のあるコンピュータの台数であり、感染コンピュータ名は、ワームに感染した可能性のあるコンピュータの名称である。感染コンピュータＩＰアドレスは、ワームに感染した可能性のあるコンピュータのＩＰアドレスである。

【００７８】

スキャン速度の情報は、単位時間当たりにＳＹＮパケットが送信されたコンピュータ数（宛先ＩＰアドレス数）の情報から算出することができる。また、感染コンピュータＩＰアドレスは、ＳＹＮパケットのヘッダから取得することができ、感染台数の情報は、その感染コンピュータＩＰアドレスの数から取得することができる。感染コンピュータ名は、ＩＰアドレスとコンピュータ名とを対応付けて記憶したデータベース（図２には、図示していない。）を用意しておくことで取得することができる。最頻出宛先ポート番号は、通信ログデータ２３０ｂに含まれる最頻出宛先ポート番号であり、警告メッセージは、ユーザに判定結果を通知して注意を促すメッセージである。

【００７９】

図７の例では、ワーム判定部２４０ｂは、ネットワークセグメントＡ１０ａ内からのランダムスキャンが検出され、さらに最頻出宛先ポート番号が「８０」番であるので、ネットワークセグメントＡ１０ａ内のＷｅｂサーバが感染した可能性があることをユーザに通知する。また、ワーム判定部２４０ｂは、記憶部２３０のワームデータ２３０ｃに記憶されたワームの特徴を参照した結果、類似していると判定されたワームの情報や、ランダムスキャンの対象となったネットワークの情報などをユーザに通知する。

【００８０】

図８は、図２に示したワーム判定部２４０ｂがおこなうネットワークセグメントＡ１０ａ外からの攻撃によるワーム感染の有無を判定する処理の一例を示す図である。ここでは、ＳＹＮ　ＡＣＫパケットに異常が検出された後、ＳＹＮパケットにも異常が検出された場合を示している。図８に示すように、ワーム判定部２４０ｂは、通信ログデータ２３０ｂを参照し、各パケットのパケット数およびＩＰアドレス数が設定データ２３０ａに記憶されている閾値以上であるか否かを調べる。

【００８１】

たとえば、ワーム判定部２４０ｂは、ＳＹＮ　ＡＣＫパケット数の閾値が「１０」、送信元ＩＰアドレス数の閾値が「１０」である場合には、計測時間「１０：００：３５～１０：００：３６」においてＳＹＮ　ＡＣＫパケット数「３０」が閾値「１０」以上であり、かつ、送信元ＩＰアドレス数「３６」が閾値「１０」以上であるので、ＳＹＮ　ＡＣＫパケットの異常を検出する。また、ワーム判定部２４０ｂは、ＳＹＮパケット数の閾値が「１０」、宛先ＩＰアドレス数の閾値が「１０」である場合には、計測時間「１０：００：３７～１０：００：３８」においてＳＹＮパケット数「２２」が閾値「１０」以上であり、かつ、宛先ＩＰアドレス数「２８」が閾値「１０」以上であるので、ＳＹＮパケットの異常を検出する。

【００８２】

さらに、ワーム判定部２４０ｂは、通信情報取得部２４０ａにより取得されたＳＹＮＡＣＫパケットおよびＳＹＮパケットの最頻出宛先ポート番号の情報から、どのサービスを狙ったワームかを検出する処理をおこなう。図８の通信ログデータ２３０ｂには、取得された最頻出宛先ポート番号「８０」の情報と、監視をおこなった全パケットのうち最頻出宛先ポート番号が「８０」番であったパケットの割合の情報（「８７％」、「８７％」、「８９％」および「８６％」）とが、ＳＹＮパケット数、ＳＹＮ　ＡＣＫパケット数、宛先ＩＰアドレス数および送信元ＩＰアドレス数のそれぞれの計測項目ごとに示されている。

【００８３】

その後、ワーム判定部２４０ｂは、上記情報を基にしてワーム感染の有無を判定し、ワーム判定結果８０を出力する処理をおこなう。具体的には、ワーム判定部２４０ｂは、ＳＹＮ　ＡＣＫパケットが、ネットワークセグメントＡ１０ａ内から閾値より多く送信され、かつ、ＳＹＮ　ＡＣＫパケットの送信元ＩＰアドレス数が閾値より多いことから、ネットワークセグメントＡを除くネットワーク１２のコンピュータからネットワークセグメントＡ１０ａ内のコンピュータに対してワームによるランダムスキャンがなされていたと判定する。

【００８４】

さらに、ワーム判定部２４０ｂは、ＳＹＮパケットが、ネットワークセグメントＡ１０ａ内から閾値より多く送信され、かつ、ＳＹＮパケットの宛先ＩＰアドレス数が閾値より多いことから、上記ランダムスキャンによりネットワークセグメントＡ１０ａ内のコンピュータがワームに感染し、そのワームに感染したコンピュータからネットワークセグメントＡを除くネットワーク１２のコンピュータに対してランダムスキャンがなされていると判定し、そのワーム判定結果８０を出力する。

【００８５】

このワーム判定結果８０は、スキャン方法、最頻出宛先ポート番号および警告メッセージの情報を含んでいる。スキャン方法は、ワームがランダムスキャンをおこなう際に使用するパケットの種類を示しており、最頻出宛先ポート番号は、通信ログデータ２３０ｂに含まれる最頻出宛先ポート番号である。警告メッセージは、ユーザに判定結果を通知して注意を促すメッセージであり、ネットワークセグメントＡ１０ａ内のＷｅｂサーバが外部からのワーム攻撃により感染した可能性があることをユーザに通知する。

【００８６】

図９は、図２に示したワーム判定部がおこなう複数コンピュータのワーム感染の有無を判定する処理の一例を示す図である。ここでは、ＳＹＮパケットに異常が検出された後、

再度ＳＹＮパケットに異常が検出された場合に、再度ＳＹＮパケットに異常が検出された際の宛先ＩＰアドレス数が、前回ＳＹＮパケットに異常が検出された際の宛先ＩＰアドレス数に比べて増加した状況を示している。

【００８７】

図９に示すように、ワーム判定部２４０ｂは、通信ログデータ２３０ｂを参照し、各パケットのパケット数およびＩＰアドレス数が設定データ２３０ａに記憶されている閾値以上であるか否かを調べる。たとえば、ワーム判定部２４０ｂは、ＳＹＮパケット数の閾値が「１０」、送信元ＩＰアドレス数の閾値が「１０」である場合に、計測時間「１０：００：３７～１０：００：３８」においてＳＹＮパケット数「２２」が閾値「１０」以上であり、かつ、宛先ＩＰアドレス数「２８」が閾値「１０」以上であるので、ＳＹＮパケットの異常を検出する。また、ワーム判定部２４０ｂは、計測時間「１０：００：３９～１０：００：４０」においてＳＹＮパケット数「４９」が閾値「１０」以上であり、かつ、宛先ＩＰアドレス数「６０」が閾値「１０」以上であるので、ＳＹＮパケットの異常を再度検出する。

【００８８】

さらに、ワーム判定部２４０ｂは、通信情報取得部２４０ａにより取得されたＳＹＮパケットの最頻出宛先ポート番号の情報から、どのサービスを狙ったワームかを検出する処理をおこなう。図９の通信ログデータ２３０ｂには、取得された最頻出宛先ポート番号「８０」の情報と、監視をおこなった全パケットのうち最頻出宛先ポート番号が「８０」番であったパケットの割合の情報（「９２％」および「９５％」）とが、ＳＹＮパケット数および宛先ＩＰアドレス数のそれぞれの計測項目ごとに示されている。

【００８９】

その後、ワーム判定部２４０ｂは、上記情報を基にしてワーム感染の有無を判定し、ワーム判定結果９０を出力する処理をおこなう。具体的には、ワーム判定部２４０ｂは、ＳＹＮパケットが、ネットワークセグメントＡ１０ａ内から閾値より多く送信され、かつ、ＳＹＮパケットの宛先ＩＰアドレス数が閾値より多いことから、ネットワークセグメントＡ１０ａ内のコンピュータがワームに感染し、そのワームに感染したコンピュータからネットワークセグメントＡを除くネットワーク１２のコンピュータに対してランダムスキャンがなされていると判定する。

【００９０】

また、ワーム判定部２４０ｂは、最頻出宛先ポート番号が「８０」番であり、今回ＳＹＮパケットに異常が検出された際の宛先ＩＰアドレス数が、前回ＳＹＮパケットに異常が検出された際の宛先ＩＰアドレス数に比べて２倍以上増加したので、ネットワークセグメントＡ１０ａ内の複数のＷｅｂサーバがワームに感染したと判定し、そのワーム判定結果９０を出力する。ここでは、宛先ＩＰアドレス数が２倍以上増加した場合に複数のＷｅｂサーバが感染したと判定したが、この倍数は任意に設定できる。

【００９１】

このワーム判定結果９０は、スキャン方法、スキャン速度、感染台数、感染コンピュータ名、感染コンピュータＩＰアドレス、最頻出宛先ポート番号および警告メッセージの情報を含んでいる。スキャン方法は、ワームがランダムスキャンをおこなう際に使用するパケットの種類を示しており、スキャン速度は、１秒間にスキャンがなされた速度の情報である。感染台数は、ワームに感染したコンピュータの台数であり、感染コンピュータ名は、ワームに感染した可能性のあるコンピュータの名称である。感染コンピュータＩＰアドレスは、ワームに感染した可能性のあるコンピュータのＩＰアドレスである。図９の例では、ワームに感染した可能性のある２台分のＷｅｂサーバの感染コンピュータ名および感染コンピュータＩＰアドレスの情報が示されている。

【００９２】

最頻出宛先ポート番号は、通信ログデータ２３０ｂに含まれる最頻出宛先ポート番号であり、警告メッセージは、ユーザに判定結果を通知して注意を促すメッセージである。図９の例では、ワーム判定結果９０は、ネットワークセグメントＡ１０ａ内の複数のＷｅｂ

サーバがワームに感染した可能性があることを警告メッセージとしてユーザに通知する。

【００９３】

図２の説明に戻ると、設定データ変更部２４０ｃは、通信情報取得部２４０ａ、ワーム判定部２４０ｂまたは通信遮断部２４０ｃにより参照される設定データ２３０ａに変更がある場合に、ユーザにより入力された新規の設定を受け付け、設定項目の新たな追加や設定項目の更新、あるいはすでに設定されている設定項目の削除などをおこなって設定データ２３０ａを変更する変更部である。また、設定データ変更部２４０ｃは、監視していたＳＹＮパケットに異常が検知された場合に、設定データ２３０ａの設定を、初期設定からＳＹＮパケット異常検知後の設定に変更する処理をおこなう。

【００９４】

通信遮断部２４０ｄは、ワーム判定部２４０ｂによりパケット通信がワームによりなされたパケット通信であると判定された場合に、ワームによりなされるパケット通信を遮断する遮断部である。この遮断処理は、図３の設定データ２３０ａにおいて設定項目「遮断」が「ＯＮ」である場合におこなわれる。また、この通信遮断部２４０ｄは、図３の設定データ２３０ａの設定項目「検知から遮断までの時間」を参照し、そこに設定された時間だけ待機した後、遮断処理を開始する。

【００９５】

通信遮断部２４０ｄは、具体的には、３通りの方法でワームによるパケット通信を遮断する。図１０は、図２に示した通信遮断部２４０ｄがおこなうワームによりなされる通信を遮断する遮断処理の例を示す図である。図１０に示すように、方法１は、通信遮断部２４０ｄが、ワームに感染したと判定されたコンピュータを含んだネットワークセグメントＡ１０ａ内のすべてのコンピュータからの特定のＯｕｔｇｏｉｎｇ通信（ランダムスキャン）を遮断する方法である。この方法１では、ワームにより送信される通信パケットのプロトコルがＴＣＰベースかＵＤＰベースかの情報や、通信パケットの最頻出宛先ポート番号の情報などを参照してＯｕｔｇｏｉｎｇ通信の遮断をおこなう。その際、通信遮断部２４０ｄは、上記情報から特定される通信パケット以外の通信パケットに対しては遮断をおこなわなず、通信障害を最小限に抑制する。

【００９６】

方法２は、通信遮断部２４０ｄが、ネットワークセグメントＡ１０ａ内のワームに感染したと判定されたコンピュータからの特定のＯｕｔｇｏｉｎｇ通信（ランダムスキャン）を遮断する方法である。この方法２では、ワームにより送信される通信パケットのプロトコルがＴＣＰベースかＵＤＰベースかの情報や、ワームに感染したと判定されたコンピュータを特定する送信元ＩＰアドレス、通信パケットの最頻出宛先ポート番号の情報などを参照してＯｕｔｇｏｉｎｇ通信の遮断をおこなう。その際、通信遮断部２４０ｄは、上記情報から特定される通信パケット以外の通信パケットに対しては遮断をおこなわず、通信障害を最小限に抑制する。

【００９７】

図１１は、ワームによりなされた通信をワーム判定装置２０ａが遮断する遮断処理を説明する説明図である。図１１は、方法１または２によりＯｕｔｇｏｉｎｇ通信の遮断をおこなう場合を示している。図１１に示すように、通信遮断部２４０ｄは、監視対象としているネットワークセグメントＡ１０ａからワームによりなされたＯｕｔｇｏｉｎｇ通信を、ワーム判定装置２０ａにおいて遮断し、ネットワークセグメントＡを除くネットワーク２１にワームにより送信された通信パケットが到達するのを防止する。ワームにより送信された通信パケット以外の通信パケットは、通信遮断部２４０ｄは、ワーム判定装置２０ａを通過させ、通信障害を回避する。

【００９８】

図１０の説明に戻ると、方法３は、方法１または方法２による遮断処理の後、通信遮断部２４０ｄが、ワームに感染したと判定されたコンピュータのランダムスキャンを遠隔操作で停止する方法である。具体的には、通信遮断部２４０ｄは、ワームに感染したと判定されたコンピュータにアクセスし、ランダムスキャンをおこなっているプロセスを停止さ

せたり、ワームに感染したと判定されたコンピュータのパーソナルファイアウォール等の機能をアクティブに設定し、自装置がおこなっているランダムスキャンを自装置に遮断させる。この方法３では、ワームにより送信される通信パケットのプロトコルがＴＣＰベースかＵＤＰベースかの情報や、ワームに感染したと判定されたコンピュータを特定する送信元ＩＰアドレス、通信パケットの最頻出宛先ポート番号の情報などを参照して、遠隔操作によりランダムスキャンの遮断をおこなう。その際、通信遮断部２４０ｄは、上記情報から特定される通信パケット以外の通信パケットに対する遮断を、ワームに感染したと判定されたコンピュータがおこなわないように操作し、通信障害を最小限に抑制する。

【００９９】

図１２は、ワームによりなされた通信を感染コンピュータ自体に遮断させる遮断処理を説明する説明図である。図１２は、方法３によりランダムスキャンの遮断をおこなう場合を示している。図１２に示すように、通信遮断部２４０ｄは、監視対象としているネットワークセグメントＡ１０ａからのランダムスキャンを、ワームに感染していると判定されたコンピュータ自体に遮断させ、ネットワークセグメントＡを除くネットワーク２１にワームにより送信された通信パケットが到達するのを防止する。ワームにより送信された通信パケット以外の通信パケットに対しては、通信遮断部２４０ｄは、ワームに感染したと判定されたコンピュータが遮断をおこなわないようにそのコンピュータを操作し、通信障害を回避する。なお、ここでは、方法１または２による遮断処理の後に方法３による遮断処理をおこなうこととしたが、方法３による遮断処理を単独でおこなうこととしてもよい。

【０１００】

ここで、特許請求の範囲または後述の付記における「通信情報取得手段」および「通信情報取得手順」・「通信情報取得工程」は、図２に示した通信情報取得部２４０ａおよび通信情報取得部２４０ａがおこなう手順・工程に対応し、「ワーム判定手段」および「ワーム判定手順」・「ワーム判定工程」は、ワーム判定部２４０ｂおよびワーム判定部２４０ｂがおこなう手順・工程に対応し、「設定情報変更手順」は、設定データ変更部２４０ｃがおこなう手順に対応し、「通信遮断手段」および「通信遮断手順」・「通信遮断工程」は、通信遮断部２４０ｄおよび通信遮断部２４０ｄがおこなう手順・工程に対応する。

【０１０１】

また、特許請求の範囲または後述の付記における「情報の取得に係る設定情報」は、図３に示した「ＳＹＮパケットの計測単位時間」、「ＳＹＮ　ＡＣＫパケットの計測単位時間」、「ＵＤＰパケットの計測単位時間」、「ＩＣＭＰ（ｒｅｑｕｅｓｔ）パケットの計測単位時間」、「ＩＣＭＰ（ｒｅｐｌｙ）パケットの計測単位時間」、「宛先ＩＰアドレスの計測単位時間」、「送信元ＩＰアドレスの計測単位時間」、「宛先ポート番号の参照」、「監視場所」、「監視するネットワークの方向」の各設定項目の情報に対応し、「通信がワームによりなされた通信か否かを規定する判定基準」は、「ＳＹＮパケット数の閾値」、「ＳＹＮ　ＡＣＫパケット数の閾値」、「ＵＤＰパケットの閾値」、「ＩＣＭＰ（ｒｅｑｕｅｓｔ）パケットの閾値」、「ＩＣＭＰ（ｒｅｐｌｙ）パケットの閾値」、「宛先ＩＰアドレス数の閾値」、「送信元ＩＰアドレス数の閾値」に対応する。

【０１０２】

また、特許請求の範囲または後述の付記における「コンピュータに係る情報」は、図６、図７または図９に示したワーム判定結果６０、７０または９０における「スキャン元ＩＰアドレス」、「感染台数」、「感染コンピュータ名」および「感染コンピュータＩＰアドレス」などに対応し、「通信状況に係る情報」は、図６～図９に示したワーム判定結果６０、７０、８０または９０における「スキャン方法」、「最頻出宛先ポート番号」、警告メッセージ、「スキャン速度」などに対応し、「ログ」は、図２に示した通信ログデータ２３０ｂに対応する。

【０１０３】

つぎに、本実施例に係るワーム判定装置２０ａのハードウェア構成について説明する。図１３は、本実施例に係るワーム判定装置２０ａのハードウェア構成について説明するブ

ロック図である。図１３に示すように、このワーム判定装置２０ａは、キーボード１３０、ディスプレイ１３１、ＣＰＵ１３２、ＲＡＭ１３３、ＨＤＤ１３４、ＲＯＭ１３６、ネットワークＩ／Ｆ１３７をバス１３８で接続した構成となる。

【０１０４】

ネットワークＩ／Ｆ１３７は、ネットワークセグメントＡ１０ａまたはネットワークセグメントＡを除くネットワーク１２とワーム判定装置２０ａとの間での、ＬＡＮ２１またはネットワーク１１を介した通信処理をおこなう。

【０１０５】

また、ＨＤＤ１３４が格納および読み出し制御する記憶媒体であるハードディスク（ＨＤ）１３５には、本実施例で示されるワーム判定方法をコンピュータで実行することにより実現するワーム判定プログラム１３５ａが記憶され、実行時にＲＡＭ１３３に読み込まれた後、ＣＰＵ１３２によりプログラムが解析され、ワーム判定プロセスの実行がおこなわれる。

【０１０６】

このワーム判定プロセスが、図２に示した制御部２４０内の通信情報取得部２４０ａ、ワーム判定部２４０ｂ、設定データ変更部２４０ｃおよび通信遮断部２４０ｄの各部の機能に対応する。また、設定データ２４０ａ、通信ログデータ２４０ｂおよびワームデータ２４０ｃもＨＤ１３５に記憶され、ＲＡＭ１３３に読み込まれてＣＰＵ１３２により参照される。

【０１０７】

なお、このワーム判定プログラム１３５ａは、インターネットなどのネットワークを介して配布することができる。また、ワーム判定プログラム１３５ａは、ハードディスク、フレキシブルディスク（ＦＤ）、ＣＤ－ＲＯＭ、ＭＯ、ＤＶＤなどのコンピュータで読み取り可能な記録媒体に記録され、コンピュータによって記録媒体から読み出されることによって実行することもできる。

【０１０８】

つぎに、本実施例に係るワーム判定処理の処理手順について説明する。図１４は、本実施例に係るワーム判定処理の処理手順を示すフローチャートである。図１４に示すように、まず、ワーム判定装置２０ａの設定データ変更部２４０ｃは、設定データ２３０ａの変更がある場合に、ユーザにより入力された設定を受け付ける（ステップＳ１４０１）。

【０１０９】

続いて、通信情報取得部２４０ａは、ネットワークセグメントＡ１０ａ内のコンピュータとネットワークセグメントＡを除くネットワーク１２内のコンピュータとの間のネットワーク通信を監視し（ステップＳ１４０２）、設定データ２３０ａに設定された計測単位時間に基づいてパケットを計測する計測時刻になったか否かを調べる（ステップＳ１４０３）。

【０１１０】

パケットを計測する計測時刻にまだなっていない場合には（ステップＳ１４０３，Ｎｏ）、ステップＳ１４０２に移行してそれ以降の処理を継続する。パケットを計測する計測時刻になった場合には（ステップＳ１４０３，Ｙｅｓ）、通信情報取得部２４０ａは、パケット情報を取得し、取得した情報を通信ログデータ２３０ｂに記憶する（ステップＳ１４０４）。

【０１１１】

その後、ワーム判定部２４０ｂは、通信情報取得部２４０ａにより取得され、通信ログデータ２３０ｂに記憶された情報を基にして、ワームによるパケット通信がなされたか否かの状況を判定する処理をおこなう（ステップＳ１４０５）。この状況判定処理については、のちに図１５－１および図１５－２で詳細に説明する。

【０１１２】

そして、ワーム判定部２４０ｂが、監視対象としているパケット通信がワームによるものではないと判定した場合には（ステップＳ１４０６，Ｎｏ）、ステップＳ１４０２に移

行してそれ以降の処理を継続する。パケット通信がワームによるものと判定した場合には（ステップＳ１４０６，Ｙｅｓ）、ワーム判定部２４０ｂは、ワームのスキャン方法やスキャン速度、スキャン特徴が類似しているワームの情報などを取得して、出力する処理をおこなう（ステップＳ１４０７）。

【０１１３】

その後、通信遮断部２４０ｄは、図１０～図１２で説明したような方法で、ワームによりなされたと判定されるパケット通信を遮断する処理をおこない（ステップＳ１４０８）、このワーム判定処理を終了する。

【０１１４】

つぎに、図１４に示した状況判定処理の処理手順について説明する。図１５－１および図１５－２は、図１４に示した状況判定処理の処理手順を示すフローチャート（１）および（２）である。図１５－１に示すように、まず、ワーム判定部２４０ｂは、通信情報取得部２４０ａが取得したＳＹＮ　ＡＣＫパケット数が設定データ２３０ａに設定されたＳＹＮ　ＡＣＫパケット数の閾値よりも大きく、かつ、送信元ＩＰアドレス数が設定データ２３０ａに設定された送信元ＩＰアドレス数の閾値よりも大きいか否かを調べる（ステップＳ１５０１）。

【０１１５】

そして、ワーム判定部２４０ｂは、ＳＹＮ　ＡＣＫパケット数がＳＹＮ　ＡＣＫパケット数の閾値よりも大きく、かつ、送信元ＩＰアドレス数が送信元ＩＰアドレス数の閾値よりも大きい場合には（ステップＳ１５０１，Ｙｅｓ）、ネットワークセグメントＡ１０ａ外からのワームスキャンがあると判定し（ステップＳ１５０２）、図１５－２に示されるように、判定結果を通信ログデータ２３０ｂに記憶して（ステップＳ１５１１）、この状況判定処理を終了する。

【０１１６】

ステップＳ１５０１において、ＳＹＮ　ＡＣＫパケット数がＳＹＮ　ＡＣＫパケット数の閾値よりも大きいという条件、または、送信元ＩＰアドレス数が送信元ＩＰアドレス数の閾値よりも大きいという条件のいずれかが満足されない場合には（ステップＳ１５０１，Ｎｏ）、ワーム判定部２４０ｂは、通信情報取得部２４０ａが取得したＳＹＮパケット数が設定データ２３０ａに設定されたＳＹＮパケット数の閾値よりも大きく、かつ、宛先ＩＰアドレス数が設定データ２３０ａに設定された宛先ＩＰアドレス数の閾値よりも大きいか否かを調べる（ステップＳ１５０３）。

【０１１７】

そして、ＳＹＮパケット数がＳＹＮパケット数の閾値よりも大きいという条件、または、宛先ＩＰアドレス数が宛先ＩＰアドレス数の閾値よりも大きいという条件のいずれかが満足されない場合には（ステップＳ１５０３，Ｎｏ）、ネットワークセグメントＡ１０ａ外からのワームスキャンはないと判定し（ステップＳ１５０４）、図１５－２に示されるように、判定結果を通信ログデータ２３０ｂに記憶して（ステップＳ１５１１）、この状況判定処理を終了する。

【０１１８】

ＳＹＮパケット数がＳＹＮパケット数の閾値よりも大きく、かつ、宛先ＩＰアドレス数が宛先ＩＰアドレス数の閾値よりも大きい場合には（ステップＳ１５０３，Ｙｅｓ）、ワーム判定部２４０ｂは、ネットワークセグメントＡ１０ａ外からのワームスキャンがあると過去の所定の時間内に判定されたか否かを調べる（ステップＳ１５０５）。過去の所定の時間内とは、たとえば、５分前から現時点までの間などである。

【０１１９】

ネットワークセグメントＡ１０ａ外からのワームスキャンがあると過去の所定の時間内に判定された場合には（ステップＳ１５０５，Ｙｅｓ）、ワーム判定部２４０ｂは、図１５－２に示されるように、ネットワークセグメントＡ１０ａ内のコンピュータがネットワークセグメントＡ１０ａ外からのパケット通信によりワームに感染したと判定する（ステップＳ１５０６）。

【０１２０】
ネットワークセグメントＡ１０ａ外からのワームスキャンがあると過去の所定の時間内に判定されなかった場合には（ステップＳ１５０５，Ｎｏ）、ワーム判定部２４０ｂは、図１５－２に示されるように、ネットワークセグメントＡ１０ａ内のコンピュータがネットワークセグメントＡ１０ａ外からのパケット通信以外の原因でワームに感染したと判定する（ステップＳ１５０７）。ここで、ネットワークセグメントＡ１０ａ外からのパケット通信以外の原因とは、ネットワークセグメントＡ１０ａ内のコンピュータが、フレキシブルディスク（ＦＤ）やＣＤ－ＲＯＭなどの記憶媒体からワームに感染した場合などである。

【０１２１】
ステップＳ１５０６またはステップＳ１５０７の判定処理ののち、ワーム判定部２４０ｂは、今回検出した宛先ＩＰアドレス数が、過去の所定の時間内に検出した宛先ＩＰアドレス数の最大値を２倍した数以上であるか否かを調べる（ステップＳ１５０８）。そして、今回検出した宛先ＩＰアドレス数が、過去の所定の時間内に検出した宛先ＩＰアドレス数の最大値を２倍した数以上である場合には（ステップＳ１５０８，Ｙｅｓ）、ネットワークセグメントＡ１０ａ内の複数のコンピュータがワームに感染したと判定し（ステップＳ１５０９）、設定データ変更部２４０ｃは、通信情報取得部２４０ａ、ワーム判定部２４０ｂまたは通信遮断部２４０ｄにより参照される設定データ２３０ａの設定を、初期設定からＳＹＮパケット異常検知後の設定に変更する処理をおこなう（ステップＳ１５１０）。

【０１２２】
ステップＳ１５０８において、今回検出した宛先ＩＰアドレス数が、過去の所定の時間内に検出した宛先ＩＰアドレス数の最大値を２倍した数以上でない場合には（ステップＳ１５１０）、ステップＳ１５１０に移行して、設定データ変更部２４０ｃは、設定データ２３０ａの設定を、初期設定からＳＹＮパケット異常検知後の設定に変更する処理をおこなう。その後、ワーム判定部２４０ｂは、判定結果を通信ログデータ２３０ｂに記憶し、この状況判定処理を終了する。

【０１２３】
上述してきたように、本実施例では、通信情報取得部２４０ａが、設定データ２３０ａに記憶された情報の取得に係る設定情報に基づいて通信パケットの通信量および通信パケットの通信アドレスに係る情報を取得し、ワーム判定部２４０ｂが、通信情報取得部２４０ａにより取得された情報および通信がワームによりなされた通信か否かを規定する、設定データ２３０ａに記憶された判定基準に係る情報に基づいて、通信がワームによりなされた通信か否かを判定することとしたので、サーバ装置かクライアント装置かに拘らず通信がワームによりなされたものか否かを容易にかつ効率的に判定することができる。

【０１２４】
また、本実施例では、通信がワームによりなされた通信と判定された場合に、設定データ変更部２４０ｃが、設定データ２３０ａに記憶された情報の取得に係る設定情報を変更し、通信情報取得部２４０ａは、変更された情報の取得に係る設定情報に基づいて通信パケットの通信量および通信パケットの通信アドレスに係る情報を取得することとしたので、通信がワームによりなされた通信と判定された場合に情報の取得に係る設定情報を変更することにより、さらに詳細にワームの挙動を監視することができる。

【０１２５】
また、本実施例では、設定データ変更部２４０ｃが、設定データ２３０ａに記憶された情報の取得に係る設定情報に新たに設定する情報の追加、または、すでに情報の取得に係る設定情報に設定されている情報の削除をおこなうこととしたので、情報の取得に係る設定情報を適宜更新することにより、ワームの挙動を適切に監視することができる。

【０１２６】
また、本実施例では、通信がワームによりなされた通信と判定された場合に、設定データ変更部２４０ｃが、設定データ２３０ａに記憶された判定基準に係る情報を変更し、通

信情報取得部２４０ａにより取得された情報および変更された判定基準に係る情報に基づいて通信がワームによりなされた通信か否かを判定することとしたので、通信がワームによりなされた通信と判定された場合に判定基準に係る情報を変更することにより、さらに厳密に通信がワームによりなされた通信か否かを判定することができる。

【０１２７】

また、本実施例では、設定データ変更部２４０ｃが、設定データ２３０ａに記憶された判定基準に係る情報に新たに設定する情報の追加、または、すでに判定基準に係る情報に設定されている情報の削除をおこなうこととしたので、判定基準に係る情報を適宜更新することにより、通信がワームによりなされたものか否かを適切に判定できる。

【０１２８】

また、本実施例では、ワーム判定部２４０ｂが、通信を監視する監視対象であるネットワークセグメントＡ１０ａからネットワークセグメントＡを除くネットワーク１２に送信される通信パケットのパケット量が増加し、かつ、通信パケットの宛先アドレス数が増加した場合に、ネットワークセグメントＡ１０ａ内のコンピュータからの通信がワームによりなされた通信であると判定することとしたので、ワームによる通信がネットワークセグメントＡ１０ａ内のコンピュータからなされた場合に、それを容易にかつ効率的に判定することができる。

【０１２９】

また、本実施例では、ワーム判定部２４０ｂが、通信を監視する監視対象であるネットワークセグメントＡ１０ａ内のコンピュータからの通信がワームによりなされた通信であると以前に判定され、ネットワークセグメントＡ１０ａからネットワークセグメントＡ１０ａを除くネットワーク１２に送信される通信パケットの宛先アドレス数が、通信がワームによりなされた通信であると判定する際に、通信情報取得部２４０ａにより取得されたネットワークセグメントＡ１０ａからネットワークセグメントＡ１０ａを除くネットワーク１２に送信される通信パケットの宛先アドレス数より増加した場合に、ネットワークセグメントＡ１０ａ内のコンピュータからの通信が複数のコンピュータに感染したワームによりなされた通信であると判定することとしたので、ワームによる通信が所定のネットワークセグメントＡ１０ａ内の複数のコンピュータからなされた場合に、それを容易にかつ効率的に判定することができる。

【０１３０】

また、本実施例では、ワーム判定部２４０ｂが、通信を監視する監視対象であるネットワークセグメントＡ１０ａに対してネットワークセグメントＡを除くネットワーク１２から送信された通信パケットに対する応答通信パケットのパケット量が増加し、かつ、通信パケットの送信元アドレス数が増加した場合に、ネットワークセグメントＡ１０ａ外のコンピュータからの通信がワームによりなされた通信であると判定することとしたので、ワームによる通信が所定のネットワークセグメントＡ１０ａ外のコンピュータからなされた場合に、それを容易にかつ効率的に判定することができる。

【０１３１】

また、本実施例では、ワーム判定部２４０ｂが、通信をワームによりなされた通信と判定した場合に、通信をおこなったコンピュータに係る情報をさらに出力することとしたので、出力されたコンピュータに係る情報を基にしてワームに感染している可能性のあるコンピュータを特定することができる。

【０１３２】

また、本実施例では、ワーム判定部２４０ｂが、通信をワームによりなされた通信と判定した場合に、通信の通信状況に係る情報をさらに出力することとしたので、出力された通信状況に係る情報を基にしてワームの活動状況を知ることができる。

【０１３３】

また、本実施例では、ワーム判定部２４０ｂが、通信がワームによりなされた通信か否かを判定した結果を通信ログデータ２３０ｂとして記憶することとしたので、過去のワームによりなされた通信の状況をいつでも調べることができる。

【０１３４】
また、本実施例では、ワーム判定部２４０ｂが、通信をワームによりなされた通信と判定した場合に、ワームによりなされる通信に係るワームデータ２３０ｃに記憶された特徴とワームによりなされたと判定した通信に係る特徴とを比較することによりワームの種類を推定することとしたので、推定されたワームの種類の情報を基にしてワームの攻撃に適切に対応することができる。
【０１３５】
また、本実施例では、通信遮断部２４０ｄが、通信がワームによりなされた通信と判定された場合に、ワームによりなされる通信を遮断することとしたので、ワームの増殖を効果的に抑制することができる。
【０１３６】
また、本実施例では、通信遮断部２４０ｄが、ワームにより起動されたプロセスを停止することによりワームによりなされる通信を遮断することとしたので、ワームがおこなう処理自体を停止させることにより、ワームの増殖を効果的に抑制することができる。
【０１３７】
また、本実施例では、通信遮断部２４０ｄが、ワームによりなされる通信をワームが存在していると判定されるコンピュータのファイアウォール機能を有効にすることにより遮断することとしたので、ワームによりなされる通信をワームに感染しているコンピュータに遮断させることにより、ワームの増殖を効果的に抑制することができる。
【０１３８】
さて、これまで本発明の実施の形態について説明したが、本発明は上述した実施の形態以外にも、上記特許請求の範囲に記載した技術的思想の範囲内において種々の異なる実施例にて実施されてもよいものである。
【０１３９】
例えば、本実施例では、ここでは、ワーム判定装置２０ａをネットワークセグメントＡ１０ａにＬＡＮ２１を介して接続することとしたが、本発明はこれに限定されるものではなく、ワーム判定装置２０ａをネットワークセグメントＡ１０ａ内のコンピュータに直結することとしてもよい。また、ネットワークセグメントＡ１０ａがコンピュータを一台のみ含む場合に、ワーム判定プログラムをそのコンピュータに導入し、そのコンピュータがネットワークセグメントＡ１０ａに係る通信を監視してワーム判定処理をおこなうこととしてもよい。
【０１４０】
また、ＳＹＮパケットとＳＹＮ　ＡＣＫパケットとを監視する監視する通信パケットの種類として主に取り上げて説明したが、本発明はこれに限定されるものではなく、ＵＤＰパケットやＩＣＭＰパケット、あるいはその他のプロトコルによるパケットにも本発明を同様に適用することができる。
【０１４１】
また、本実施例では、図５～図９に示したような判定方法に基づいて、通信がワームによりなされた通信か否かを判定することとしたが、本発明はこれに限定されるものではなく、通信パケットの通信量および通信パケットの通信アドレスに係る情報を用いた他のさまざまな判定方法を適用することとしてもよい。
【０１４２】
また、本実施例において説明した各処理のうち、自動的におこなわれるものとして説明した処理の全部または一部を手動的におこなうこともでき、あるいは、手動的におこなわれるものとして説明した処理の全部または一部を公知の方法で自動的におこなうこともできる。この他、上記文書中や図面中で示した処理手順、制御手順、具体的名称、各種のデータやパラメータを含む情報については、特記する場合を除いて任意に変更することができる。
【０１４３】
また、図示した各装置の各構成要素は機能概念的なものであり、必ずしも物理的に図示

のように構成されていることを要しない。すなわち、ワーム判定装置２０ａ～２０ｄの分散・統合の具体的形態は図示のものに限られず、その全部または一部を、各種の負荷や使用状況などに応じて、任意の単位で機能的または物理的に分散・統合して構成することができる。さらに、ワーム判定装置２０ａ～２０ｄによりおこなわれる各処理機能は、その全部または任意の一部が、ＣＰＵおよび当該ＣＰＵにて解析実行されるプログラムにて実現され、あるいは、ワイヤードロジックによるハードウェアとして実現され得る。

【０１４４】

（付記１）ネットワークに接続された所定のネットワークセグメントに係る通信を監視して該通信がワームによりなされた通信か否かを判定するワーム判定プログラムであって、

情報の取得に係る設定情報に基づいて通信パケットの通信量および該通信パケットの通信アドレスに係る情報を取得する通信情報取得手順と、

前記通信情報取得手順により取得された情報および前記通信がワームによりなされた通信か否かを規定する判定基準に係る情報に基づいて前記通信がワームによりなされた通信か否かを判定するワーム判定手順と、

をコンピュータに実行させることを特徴とするワーム判定プログラム。

【０１４５】

（付記２）前記ワーム判定手順により前記通信がワームによりなされた通信と判定された場合に、前記情報の取得に係る設定情報を変更する設定情報変更手順をさらに含み、前記通信情報取得手順は、前記情報取得設定変更手順により変更された情報の取得に係る設定情報に基づいて通信パケットの通信量および該通信パケットの通信アドレスに係る情報を取得することを特徴とする付記１に記載のワーム判定プログラム。

【０１４６】

（付記３）前記ワーム判定手順により前記通信がワームによりなされた通信と判定された場合に、前記判定基準に係る情報を変更する判定基準情報変更手順をさらに含み、前記ワーム判定手順は、前記通信情報取得手順により取得された情報および前記判定基準情報変更手順により変更された判定基準に係る情報に基づいて前記通信がワームによりなされた通信か否かを判定することを特徴とする付記１または２に記載のワーム判定プログラム。

【０１４７】

（付記４）前記ワーム判定手順は、通信を監視する監視対象である前記所定のネットワークセグメントから該所定のネットワークセグメント外部に送信される通信パケットのパケット量が増加し、かつ、該通信パケットの宛先アドレス数が増加した場合に、前記所定のネットワークセグメント内のコンピュータからの通信がワームによりなされた通信であると判定することを特徴とする付記１、２または３に記載のワーム判定プログラム。

【０１４８】

（付記５）前記ワーム判定手順は、通信を監視する監視対象である前記所定のネットワークセグメント内のコンピュータからの通信がワームによりなされた通信であると以前に判定され、該所定のネットワークセグメントから該所定のネットワークセグメント外部に送信される通信パケットの宛先アドレス数が、前記通信がワームによりなされた通信であると判定する際に前記通信情報取得手段により取得された該所定のネットワークセグメントから該所定のネットワークセグメント外部に送信される通信パケットの宛先アドレス数より増加した場合に、該所定のネットワークセグメント内のコンピュータからの通信が複数のコンピュータに感染したワームによりなされた通信であると判定することを特徴とする付記４に記載のワーム判定プログラム。

【０１４９】

（付記６）前記ワーム判定手順は、通信を監視する監視対象である前記所定のネットワークセグメントに対して該所定のネットワークセグメント外部から送信された通信パケットに対する応答通信パケットのパケット量が増加し、かつ、該通信パケットの送信元アドレス数が増加した場合に、前記所定のネットワークセグメント外部のコンピュータからの通信がワームによりなされた通信であると判定することを特徴とする付記１～５のいずれか１つに記載のワーム判定プログラム。

【０１５０】
（付記７）前記ワーム判定手順は、前記通信をワームによりなされた通信と判定した場合に、該通信をおこなったコンピュータもしくは通信状況に係る情報をさらに出力することを特徴とする付記１～６のいずれか１つに記載のワーム判定プログラム。
【０１５１】
（付記８）前記ワーム判定手順は、前記通信をワームによりなされた通信と判定した場合に、ワームによりなされる通信に係るあらかじめ登録された特徴とワームによりなされたと判定した通信に係る特徴とを比較することにより前記ワームの種類を推定することを特徴とする付記１～７のいずれか１つに記載のワーム判定プログラム。
【０１５２】
（付記９）前記ワーム判定手順により前記通信がワームによりなされた通信と判定された場合に、該ワームによりなされる通信を遮断する通信遮断手順を含んだことを特徴とする付記１～８のいずれか１つに記載のワーム判定プログラム。
【０１５３】
（付記１０）前記通信遮断手順は、ワームにより起動されたプロセスを停止することによりワームによりなされる通信を遮断することを特徴とする付記９に記載のワーム判定プログラム。
【０１５４】
（付記１１）前記通信遮断手順は、ワームによりなされる通信を該ワームが存在していると判定されるコンピュータのファイアウォール機能を有効にすることにより遮断することを特徴とする付記９に記載のワーム判定プログラム。
【０１５５】
（付記１２）ネットワークに接続された所定のネットワークセグメントに係る通信を監視して該通信がワームによりなされた通信か否かを判定するワーム判定プログラムを記録したコンピュータ読み取り可能な記録媒体であって、
情報の取得に係る設定情報に基づいて通信パケットの通信量および該通信パケットの通信アドレスに係る情報を取得する通信情報取得手順と、
前記通信情報取得手順により取得された情報および前記通信がワームによりなされた通信か否かを規定する判定基準に係る情報に基づいて前記通信がワームによりなされた通信か否かを判定するワーム判定手順と、
をコンピュータに実行させるワーム判定プログラムを記録したことを特徴とするコンピュータ読み取り可能な記録媒体。
【０１５６】
（付記１３）ネットワークに接続された所定のネットワークセグメントに係る通信を監視して該通信がワームによりなされた通信か否かを判定するワーム判定方法であって、
情報の取得に係る設定情報に基づいて通信パケットの通信量および該通信パケットの通信アドレスに係る情報を取得する通信情報取得工程と、
前記通信情報取得工程により取得された情報および前記通信がワームによりなされた通信か否かを規定する判定基準に係る情報に基づいて前記通信がワームによりなされた通信か否かを判定するワーム判定工程と、
を含んだことを特徴とするワーム判定方法。
【０１５７】
（付記１４）ネットワークに接続された所定のネットワークセグメントに係る通信を監視して該通信がワームによりなされた通信か否かを判定するワーム判定装置であって、
情報の取得に係る設定情報に基づいて通信パケットの通信量および該通信パケットの通信アドレスに係る情報を取得する通信情報取得手段と、
前記通信情報取得手段により取得された情報および前記通信がワームによりなされた通信か否かを規定する判定基準に係る情報に基づいて前記通信がワームによりなされた通信か否かを判定するワーム判定手段と、
を備えたことを特徴とするワーム判定装置。

【産業上の利用可能性】

【０１５８】

以上のように、本発明に係るワーム判定プログラム、ワーム判定プログラムを記憶したコンピュータ読み取り可能な記憶媒体、ワーム判定方法およびワーム判定装置は、サーバ装置かクライアント装置かに拘らず通信がワームによりなされたものか否かを容易にかつ効率的に判定することが必要なワーム判定システムに有用である。

【図面の簡単な説明】

【０１５９】

【図１】本実施例に係るワーム判定システムの概念について説明する概念図である。

【図２】本実施例に係るワーム判定装置の機能的構成について説明する機能ブロック図である。

【図３】図２に示した設定データの一例を示す図である。

【図４】図２に示した通信ログデータの一例を示す図である。

【図５】図２に示したワーム判定部がおこなうパケットの種類ごとのワーム判定処理の例を示す図である。

【図６】図２に示したワーム判定部がおこなうネットワークセグメントＡ外からのワームスキャンの有無を判定する処理の一例を示す図である。

【図７】図２に示したワーム判定部がおこなうワーム感染の有無を判定する処理の一例を示す図である。

【図８】図２に示したワーム判定部がおこなうネットワークセグメントＡ外からの攻撃によるワーム感染の有無を判定する処理の一例を示す図である。

【図９】図２に示したワーム判定部がおこなう複数コンピュータのワーム感染の有無を判定する処理の一例を示す図である。

【図１０】図２に示した通信遮断部がおこなうワームによりなされる通信を遮断する遮断処理の例を示す図である。

【図１１】ワームによりなされた通信をワーム判定装置が遮断する遮断処理を説明する説明図である。

【図１２】ワームによりなされた通信を感染コンピュータ自体に遮断させる遮断処理を説明する説明図である。

【図１３】本実施例に係るワーム判定装置のハードウェア構成について説明するブロック図である。

【図１４】本実施例に係るワーム判定処理の処理手順を示すフローチャートである。

【図１５－１】図１４に示した状況判定処理の処理手順を示すフローチャート（１）である。

【図１５－２】図１４に示した状況判定処理の処理手順を示すフローチャート（２）である。

【図１６】ネットワークセグメントの概念を説明する概念図である。

【符号の説明】

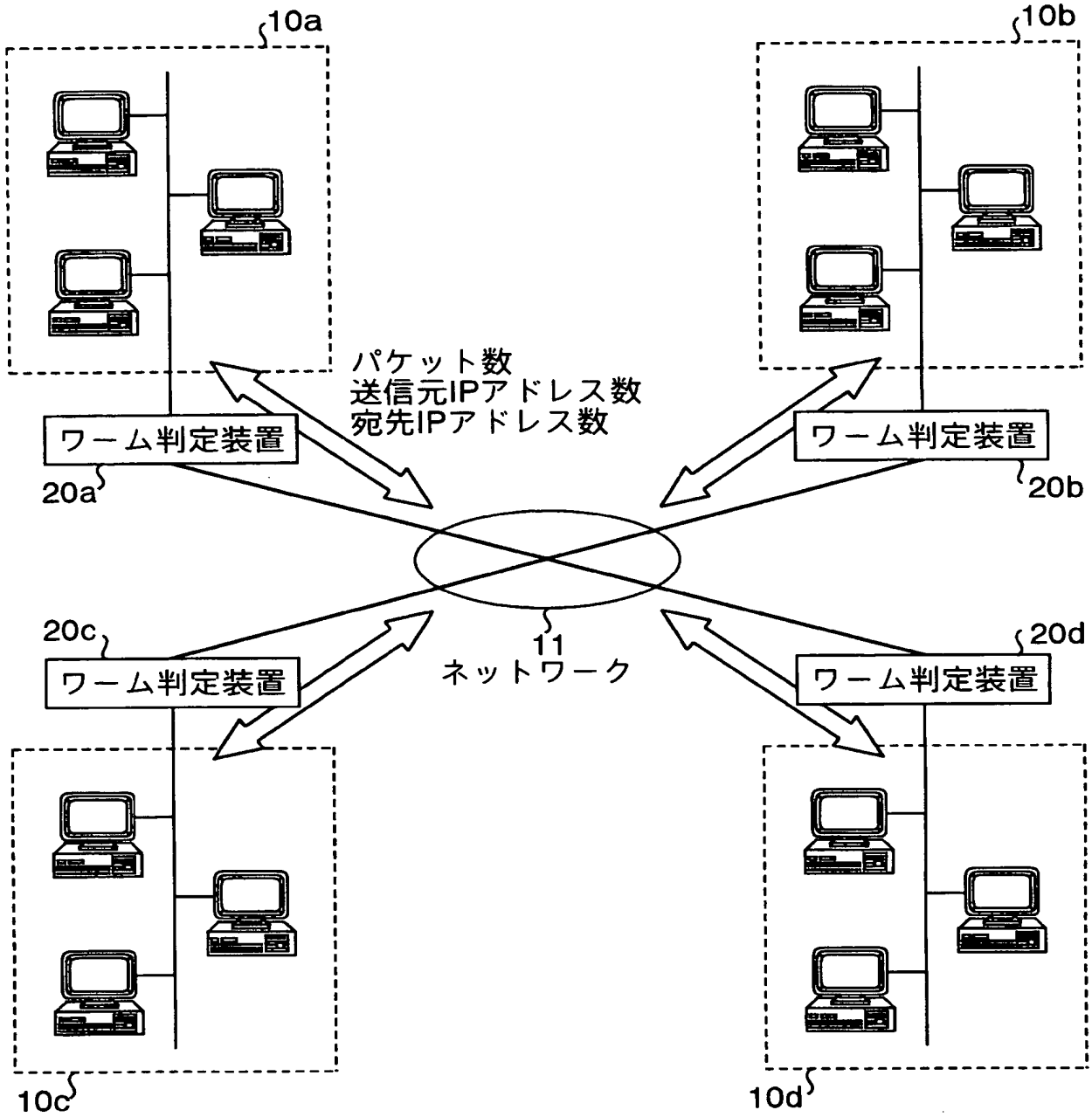
【０１６０】

１０ａ～１０ｄ、１６ａ～１６ｄ　ネットワークセグメント
１１　ネットワーク
１３０　キーボード
１３１　ディスプレイ
１３２　ＣＰＵ
１３３　ＲＡＭ
１３４　ＨＤＤ
１３５　ＨＤ
１３５ａ　ワーム判定プログラム
１３６　ＲＯＭ
１３７　ネットワークＩ／Ｆ

１３８　　バス
１７ａ～１７ｃ、２０ａ～２０ｄ　　ワーム判定装置
２００　　インターフェース部
２１　　ＬＡＮ
２１０　　入力部
２２０　　表示部
２３０　　記憶部
２３０ａ　　設定データ
２３０ｂ　　通信ログデータ
２３０ｃ　　ワームデータ
２４０　　制御部
２４０ａ　　通信情報取得部
２４０ｂ　　ワーム判定部
２４０ｃ　　設定データ変更部
２４０ｄ　　通信遮断部
６０、７０、８０、９０　　ワーム判定結果

【書類名】図面
【図１】

本実施例に係るワーム判定システムの概念について説明する概念図



【図２】

本実施例に係るワーム判定装置の機能的構成について説明する機能ブロック図

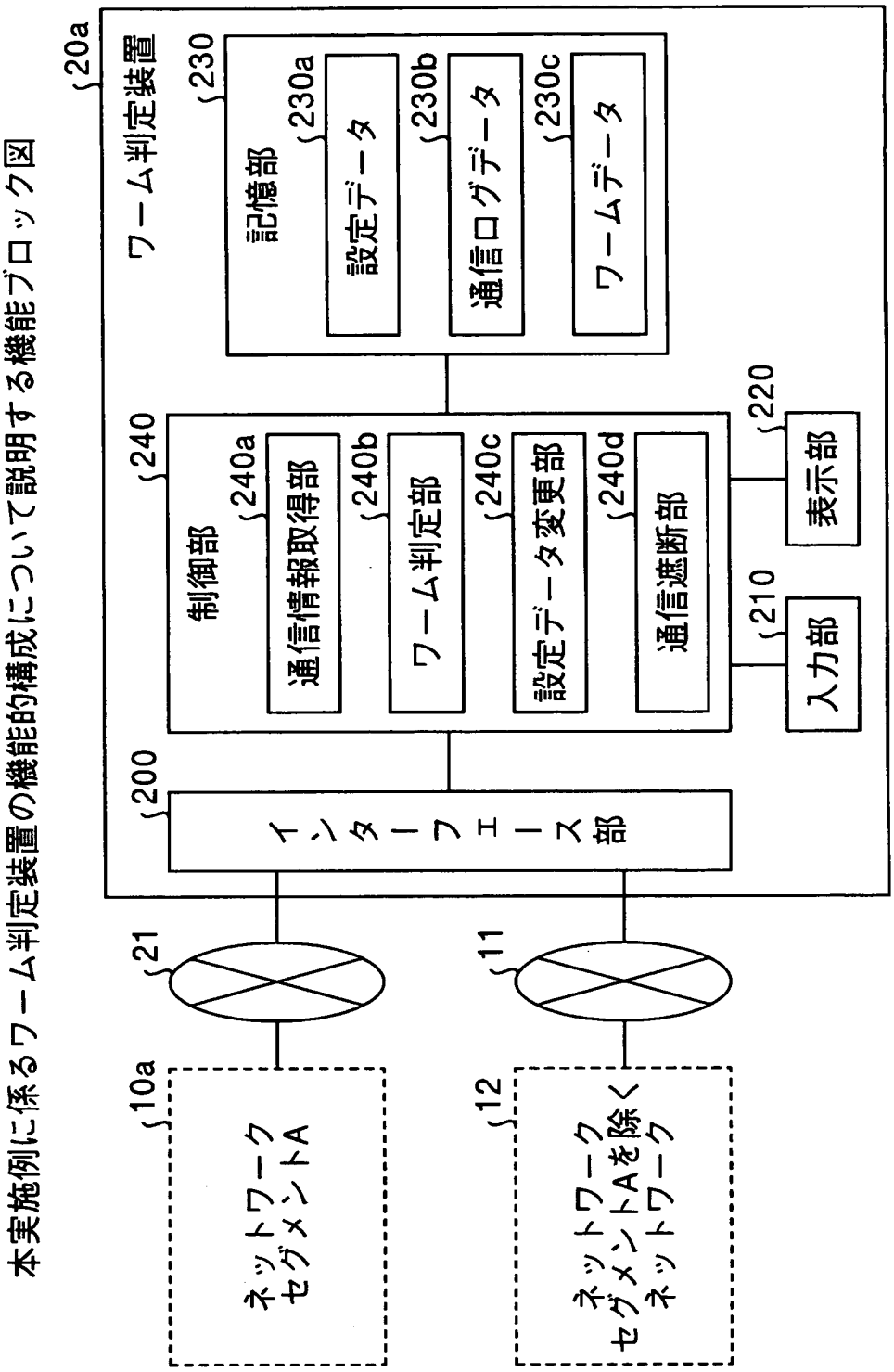


図2に示した設定データの一例を示す図

230a 設定データ

設定項目	初期設置	SYNパケット異常検知後の設定
SYNパケットの計測単位時間	1 sec	**0.1 sec**
SYN ACKパケットの計測単位時間	1 sec	1 sec
UDPパケットの計測単位時間	1 sec	1 sec
ICMP(request)パケットの計測単位時間	1 sec	1 sec
ICMP(reply)パケットの計測単位時間	1 sec	1 sec
宛先IPアドレスの計測単位時間	1 sec	**0.1 sec**
送信元IPアドレスの計測単位時間	1 sec	1 sec
宛先ポート番号の参照	OFF	**ON**
SYNパケット数の閾値	10	**2**
SYN ACKパケット数の閾値	10	10
UDPパケット数の閾値	10	10
ICMP(request)パケット数の閾値	10	10
ICMP(reply)パケット数の閾値	10	10
宛先IPアドレス数の閾値	10	**2**
送信元IPアドレス数の閾値	10	10
監視場所	Eth0	Eth0
監視するネットワークの方向	Outgoing	Outgoing
遮断	OFF	**ON**
検知から遮断までの時間	5 sec	5 sec

【図４】

図2に示した通信ログデータの一例を示す図

230b 通信ログデータ

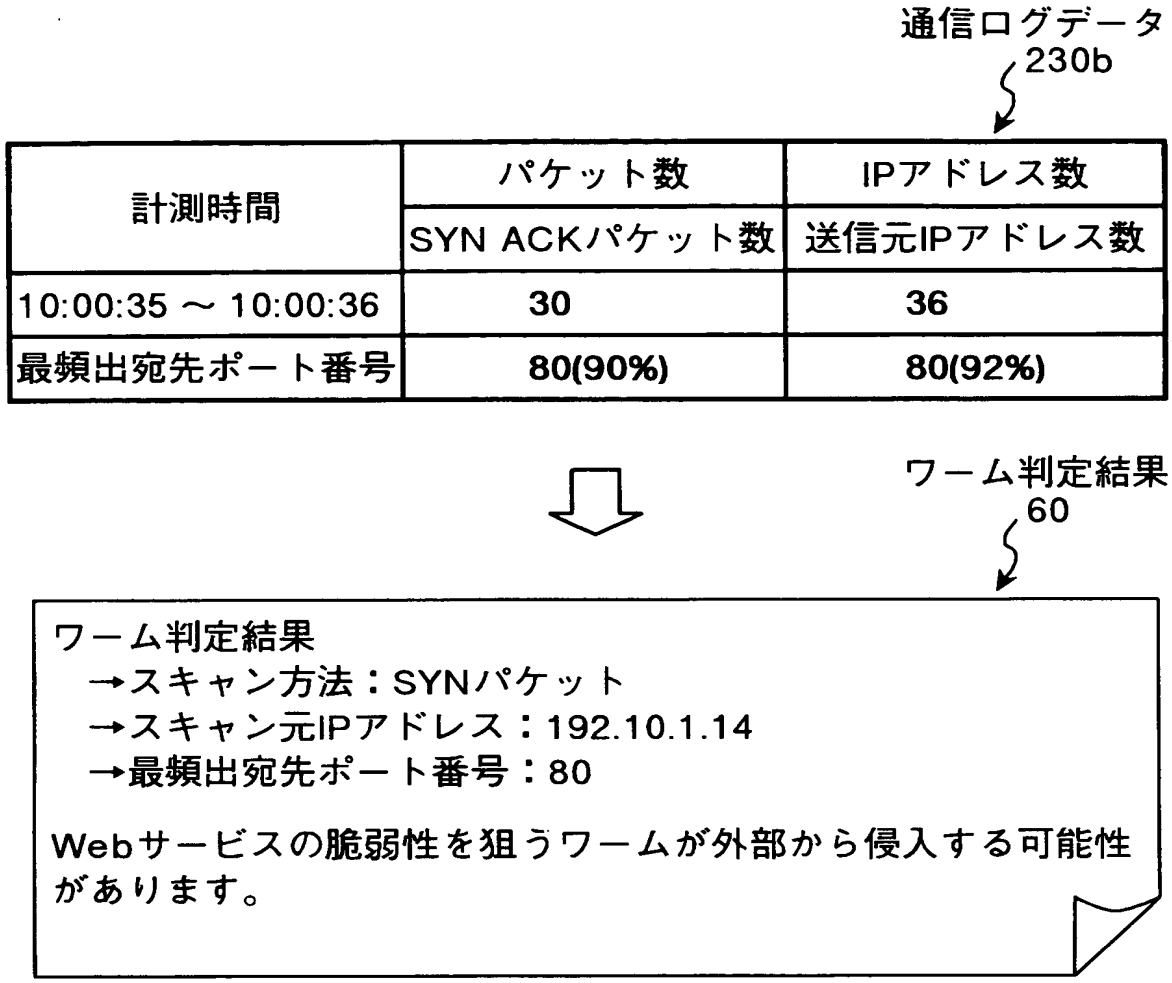
計測時間	パケット数					IPアドレス数	
	SYN パケット数	SYN ACK パケット数	UDP パケット数	ICMP (request) パケット数	ICMP (replay) パケット数	宛先 IPアドレス数	送信元 IPアドレス数
10:00:34 ～ 10:00:35	4	4	7	0	0	8	9
10:00:35 ～ 10:00:36	5	30	4	1	1	7	36
10:00:36 ～ 10:00:37	5	5	4	2	2	6	8
10:00:37 ～ 10:00:38	22	4	7	0	0	28	8
10:00:38 ～ 10:00:39	4	4	7	0	0	10	9
10:00:39 ～ 10:00:40	49	5	8	0	0	60	10
：	：	：	：	：	：	：	：

図2に示したワーム判定部がおこなうパケットの種類ごとのワーム判定処理の例を示す図

ケース番号	状況	判定	処理
1	Outgoing通信においてSYNパケット数が増加し、かつ、宛先IPアドレス数が増加。	TCPベースのワーム。	最頻出ポート番号からどのサービスを狙ったワームかを検出。80番ポートならWebサービスである。
2	Outgoing通信においてUDPパケット数が増加し、かつ、宛先IPアドレス数が増加。	UDPベースのワーム。	最頻出ポート番号からどのサービスを狙ったワームかを検出。53番ポートならDNSサービスである。
3	Outgoing通信においてICMP(request)パケット数が増加し、かつ、宛先IPアドレス数が増加。	－	その後のSYNパケットあるいはUDPパケットを監視し、TCPベースのワームか、あるいはUDPベースのワームかを判定し、最頻出ポート番号からどのサービスを狙ったワームかを検出。

【図６】

図2に示したワーム判定部がおこなうネットワークセグメントA外からのワームスキャンの有無を判定する処理の一例を示す図



【図７】

図2に示したワーム判定部がおこなう
ワーム感染の有無を判定する処理の一例を示す図

通信ログデータ
230b

計測時間	パケット数	IPアドレス数
	SYNパケット数	宛先IPアドレス数
10:00:37 ～ 10:00:38	22	28
最頻出宛先ポート番号	80(94%)	80(89%)

ワーム判定結果
70

ワーム判定結果
→スキャン方法：SYNパケット
→スキャン速度：10scan/sec
→感染台数：1台
→感染コンピュータ名：lemon
→感染コンピュータIPアドレス：192.10.3.5
→最頻出宛先ポート番号：80

・セグメント内部のWebサーバが感染した可能性があります。
・スキャン特徴がBlasterワームに似ています。
・ネットワーク192.10.4.0/24にスキャンしました。

図2に示したワーム判定部がおこなうネットワークセグメントA外からの攻撃によるワーム感染の有無を判定する処理の一例を示す図

通信ログデータ
230b

計測時間	ﾊﾟｹｯﾄ数		IPｱﾄﾞﾚｽ数	
	SYNﾊﾟｹｯﾄ数	SYN ACKﾊﾟｹｯﾄ数	宛先IPｱﾄﾞﾚｽ数	送信元IPｱﾄﾞﾚｽ数
10:00:35 ～ 10:00:36	5	30	7	36
10:00:36 ～ 10:00:37	5	5	6	8
10:00:37 ～ 10:00:38	22	4	28	8
最頻出宛先ポート番号	80(87%)	80(87%)	80(89%)	80(86%)

ワーム判定結果
80

ワーム判定結果
→スキャン方法：SYNパケット
→最頻出宛先ポート番号：80

セグメント内部のWebサーバが外部から感染した可能性があります。

【図９】

図2に示したワーム判定部がおこなう複数コンピュータの
ワーム感染の有無を判定する処理の一例を示す図

通信ログデータ
230b

計測時間	パケット数	IPアドレス数
	SYNパケット数	宛先IPアドレス数
10:00:37 ～ 10:00:38	22	28
10:00:38 ～ 10:00:39	4	10
10:00:39 ～ 10:00:40	49	60
最頻出宛先ポート番号	80(92%)	80(95%)

ワーム判定結果
90

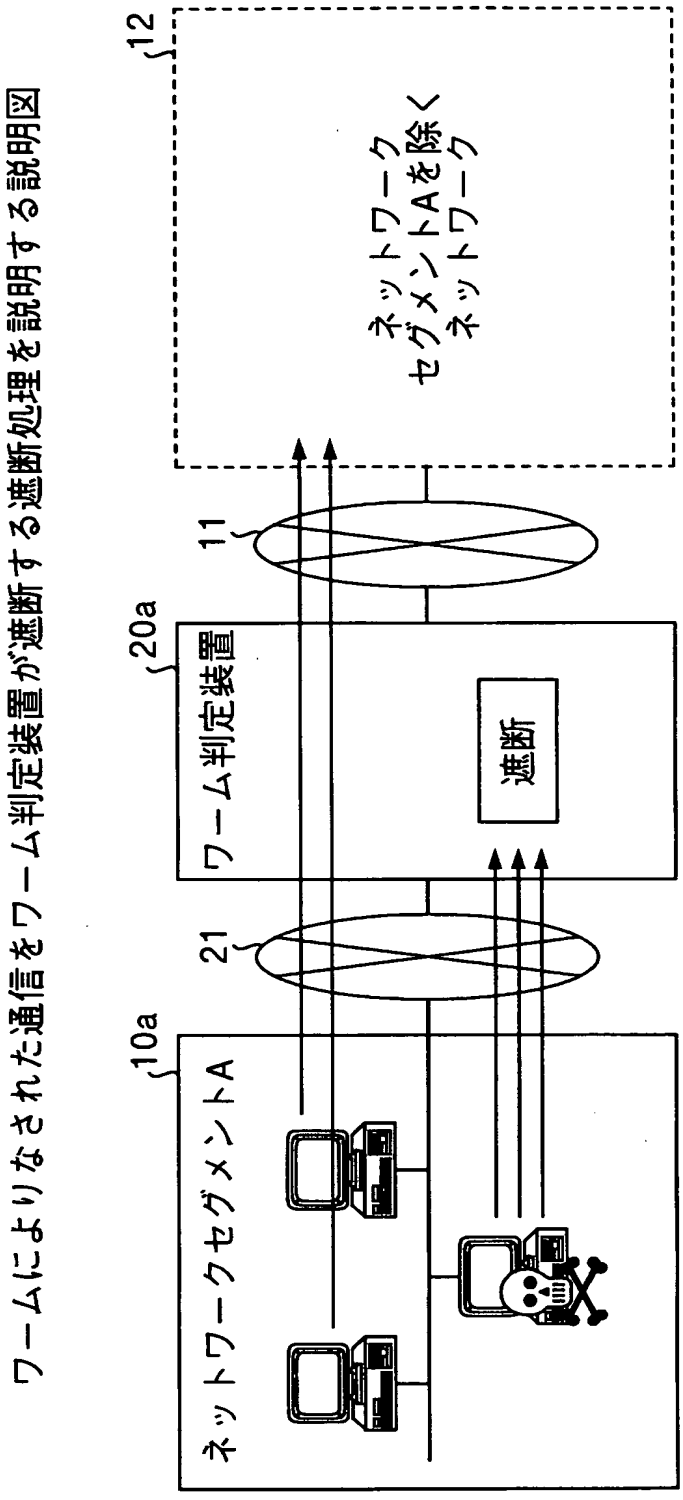
ワーム判定結果
→スキャン方法：SYNパケット
→スキャン速度：10scan/sec
→感染台数：1台→2台
→感染コンピュータ名：lemon,apple
→感染コンピュータIPアドレス：192.10.2.5,192.10.2.11
→最頻出宛先ポート番号：80

セグメント内部で複数のWebサーバが感染した可能性があります。

図2に示した通信遮断部がおこなうワームによりなされる通信の遮断処理の例を示す図

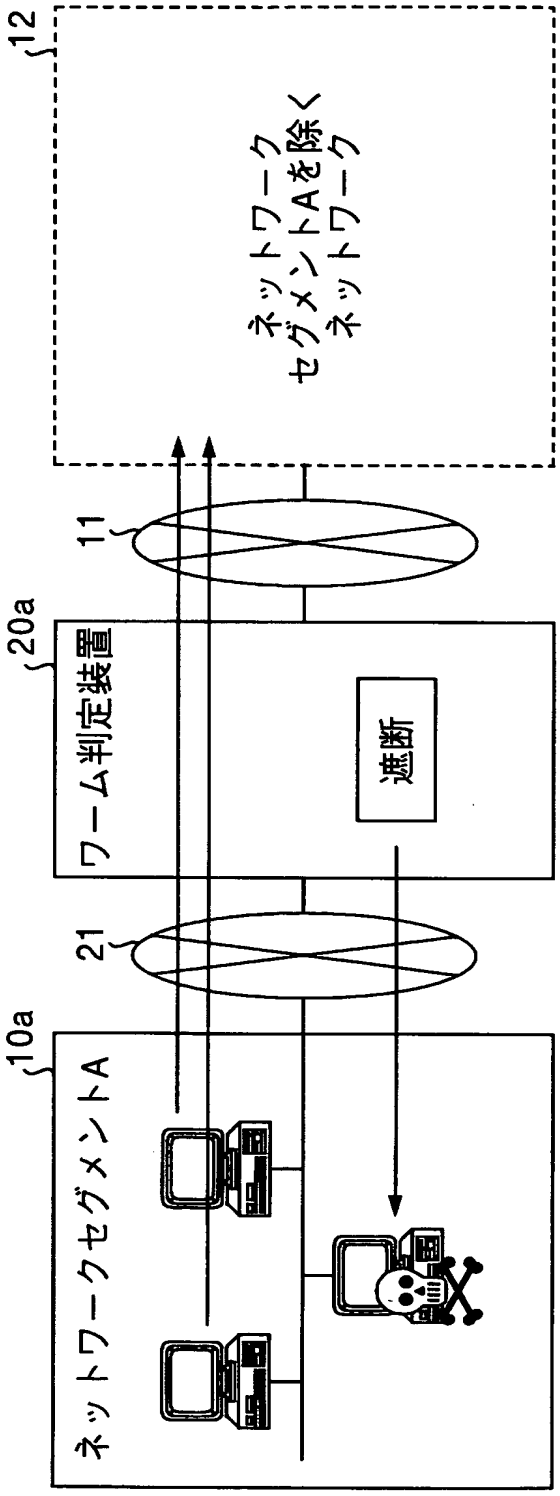
方法	処理	参照情報
1	ワームに感染したコンピュータを含んだネットワークセグメントからの特定のOutgoing通信(ランダムスキャン)を遮断。	通信プロトコル(TCP/UDP) 最頻出宛先ポート番号
2	ワームに感染したコンピュータからの特定のOutgoing通信(ランダムスキャン)を遮断。	通信プロトコル(TCP/UDP) 送信元IPアドレス 最頻出宛先ポート番号
3	方法1または2の処理後、ワームに感染したコンピュータのランダムスキャンを遠隔操作で停止(ランダムスキャンをおこなっているプロセスの停止や、パーソナルファイアウォール等による自装置のランダムスキャンの遮断等。)	通信プロトコル(TCP/UDP) 送信元IPアドレス 最頻出宛先ポート番号

【図１１】


ワームにより なされた通信をワーム判定装置が遮断する遮断処理を説明する説明図
12
ネットワーク
セグメントAを除く
ネットワーク
11
20a
ワーム判定装置
遮断
21
10a
ネットワークセグメントA

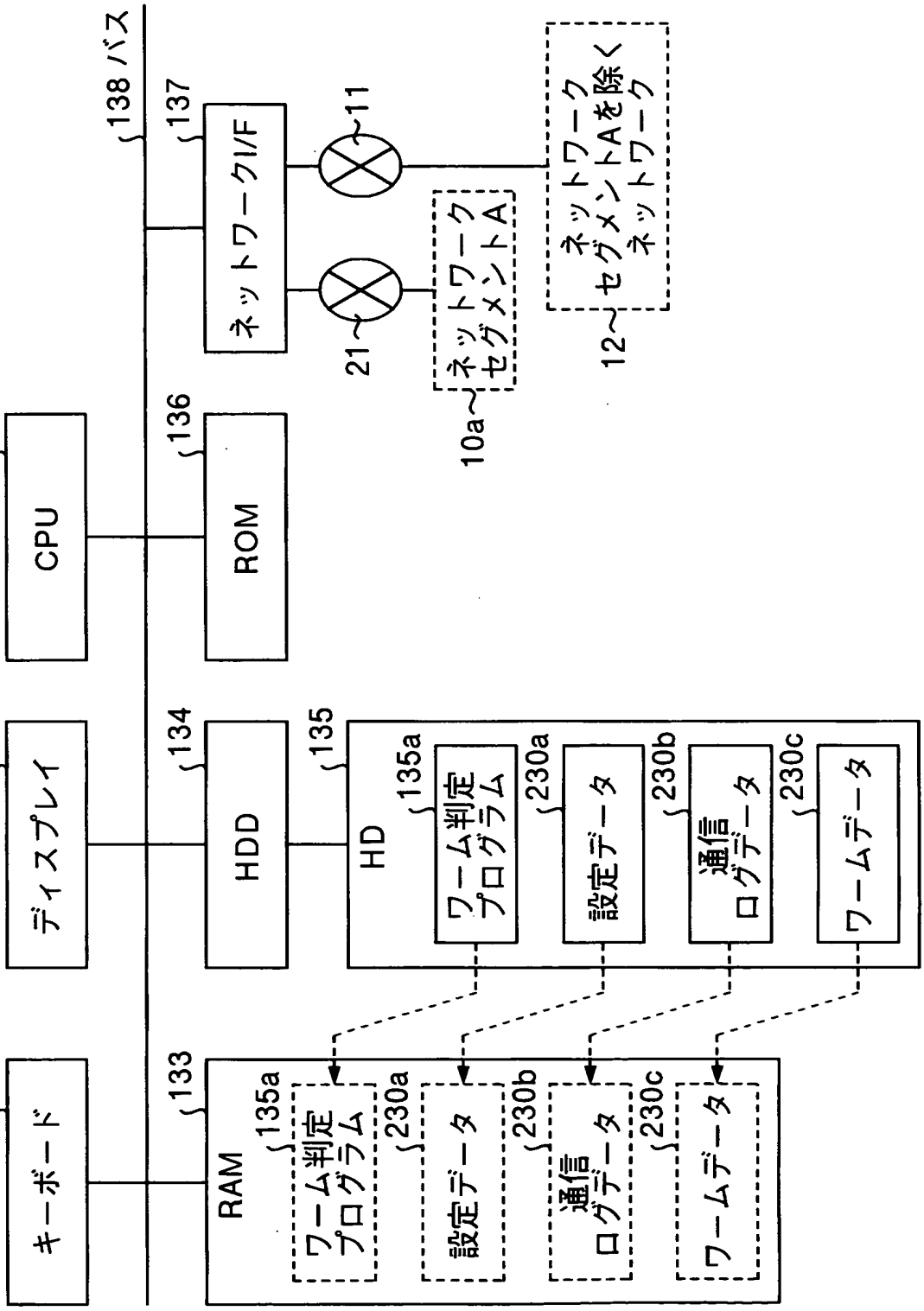
【図１２】

ワームによりなされた通信を感染コンピュータ自体に遮断させる遮断処理を説明する説明図



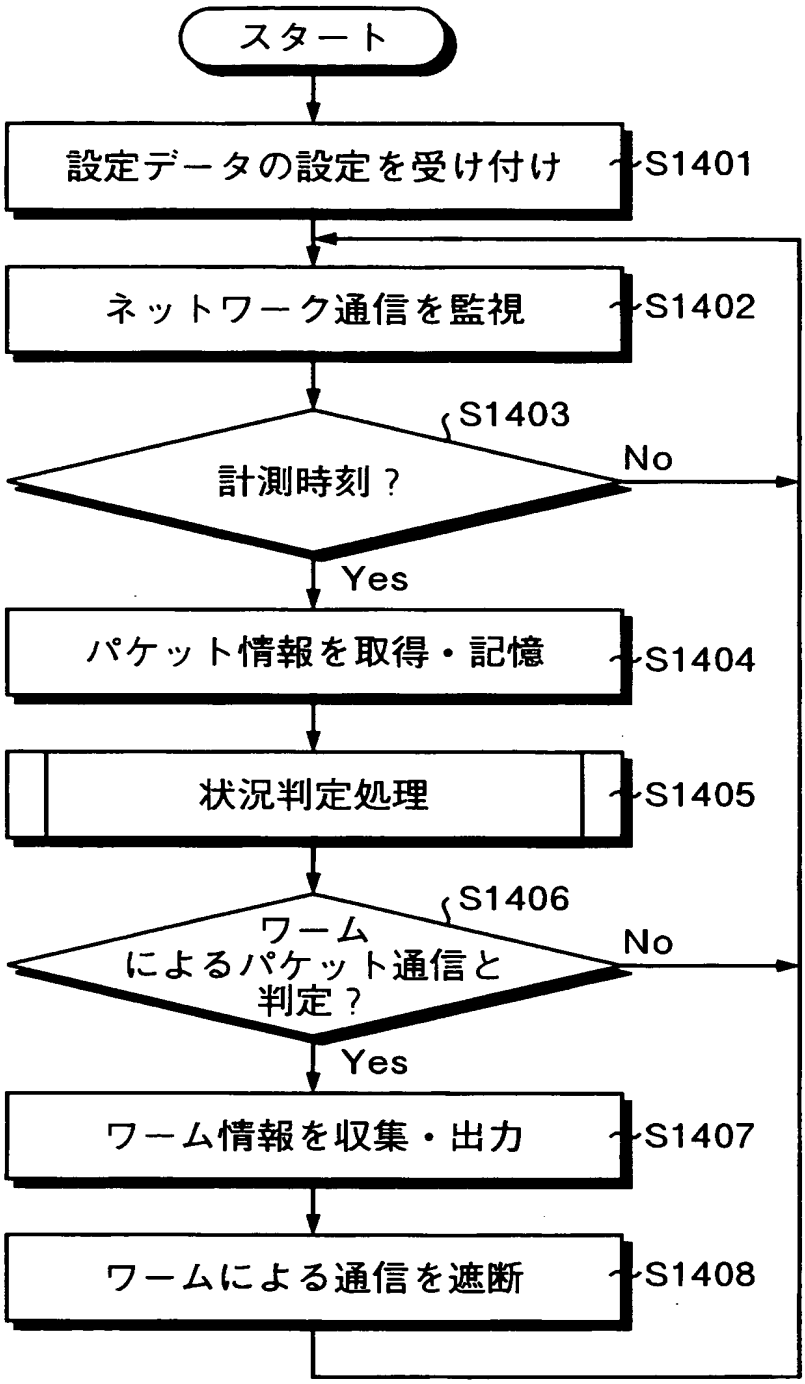
【図１３】

本実施例に係るワーム判定装置のハードウェア構成について説明するブロック図



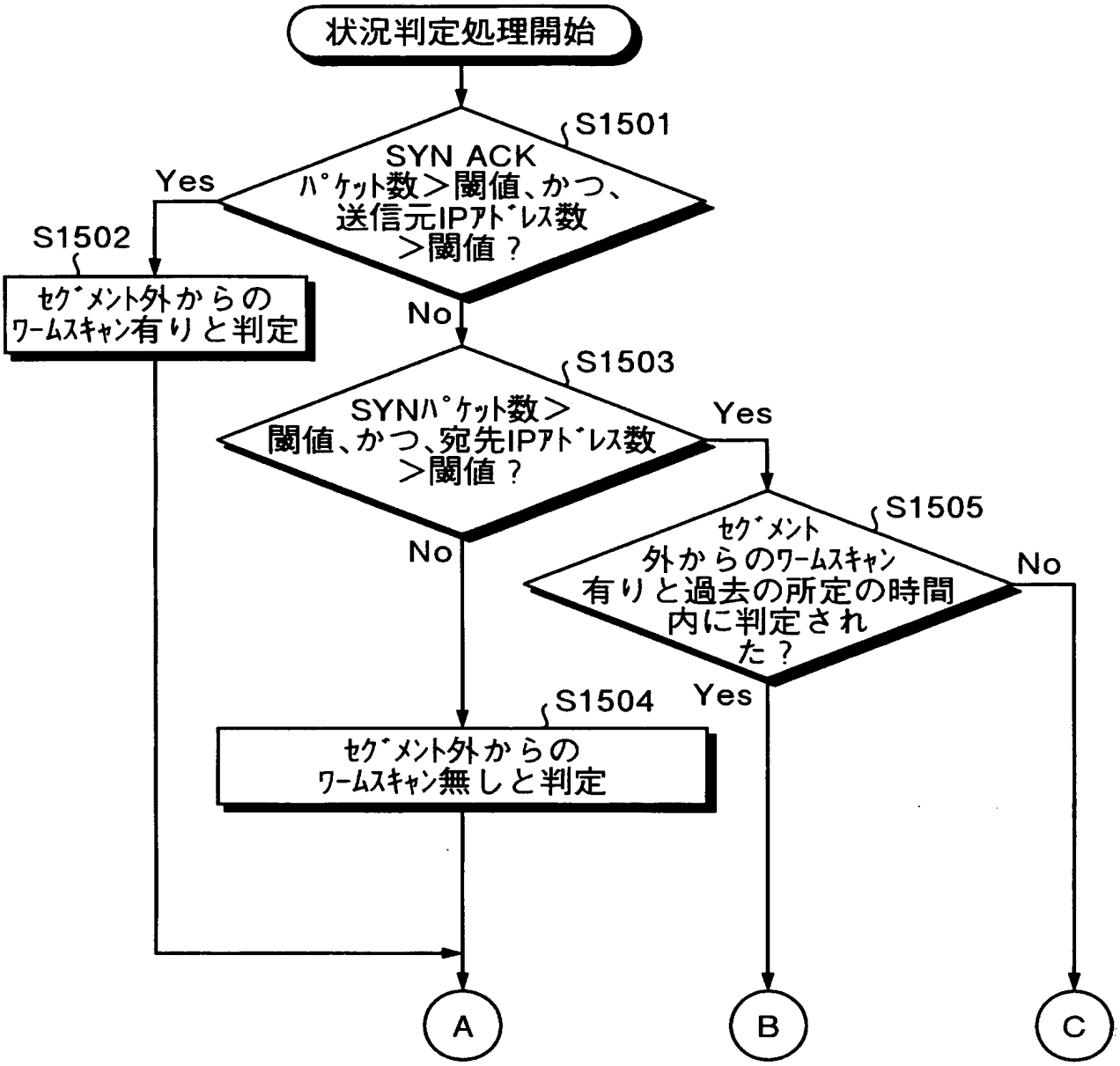
【図１４】

本実施例に係るワーム判定処理の処理手順を示すフローチャート



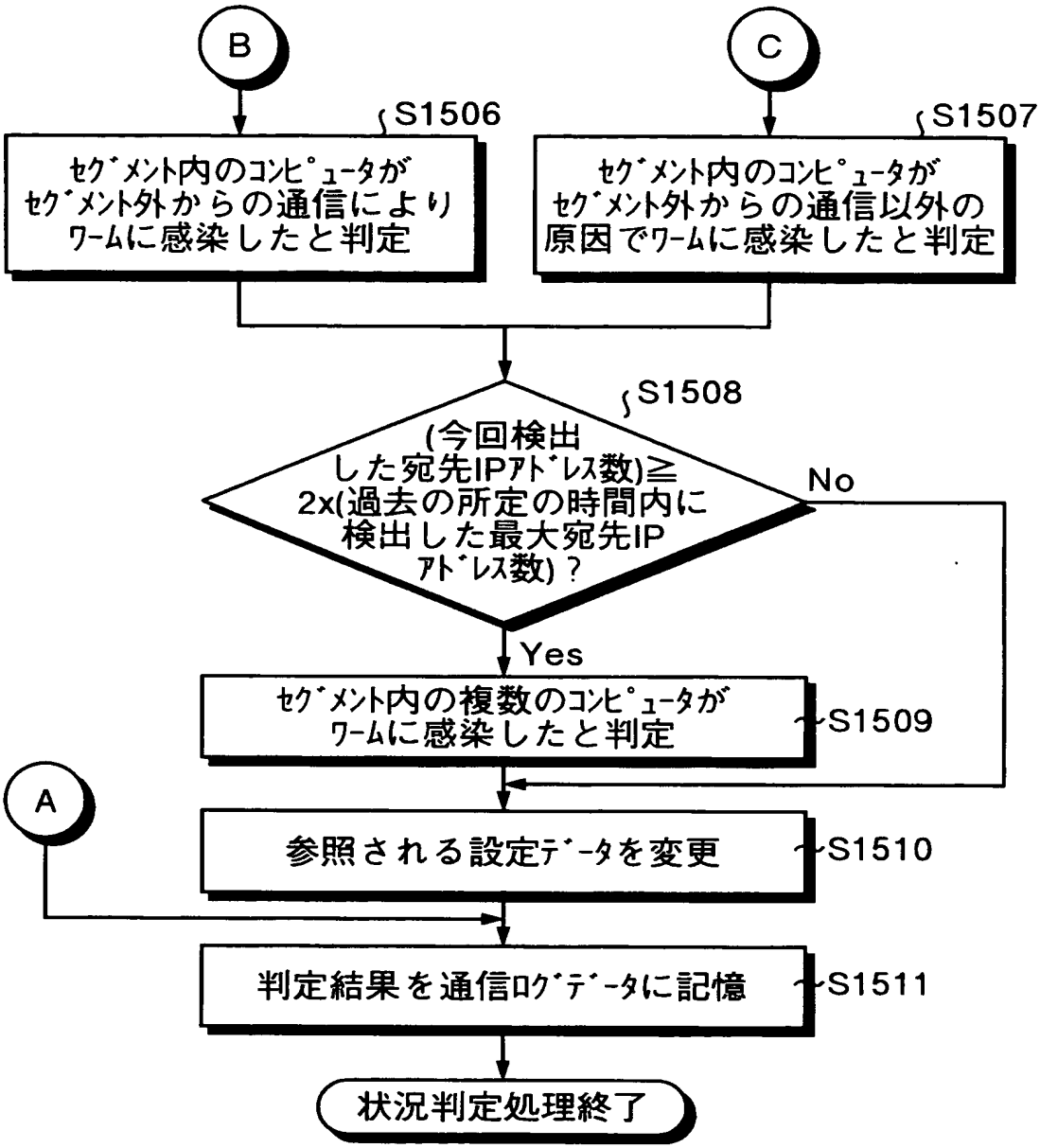
【図１５－１】

図14に示した状況判定処理の処理手順を示すフローチャート(1)



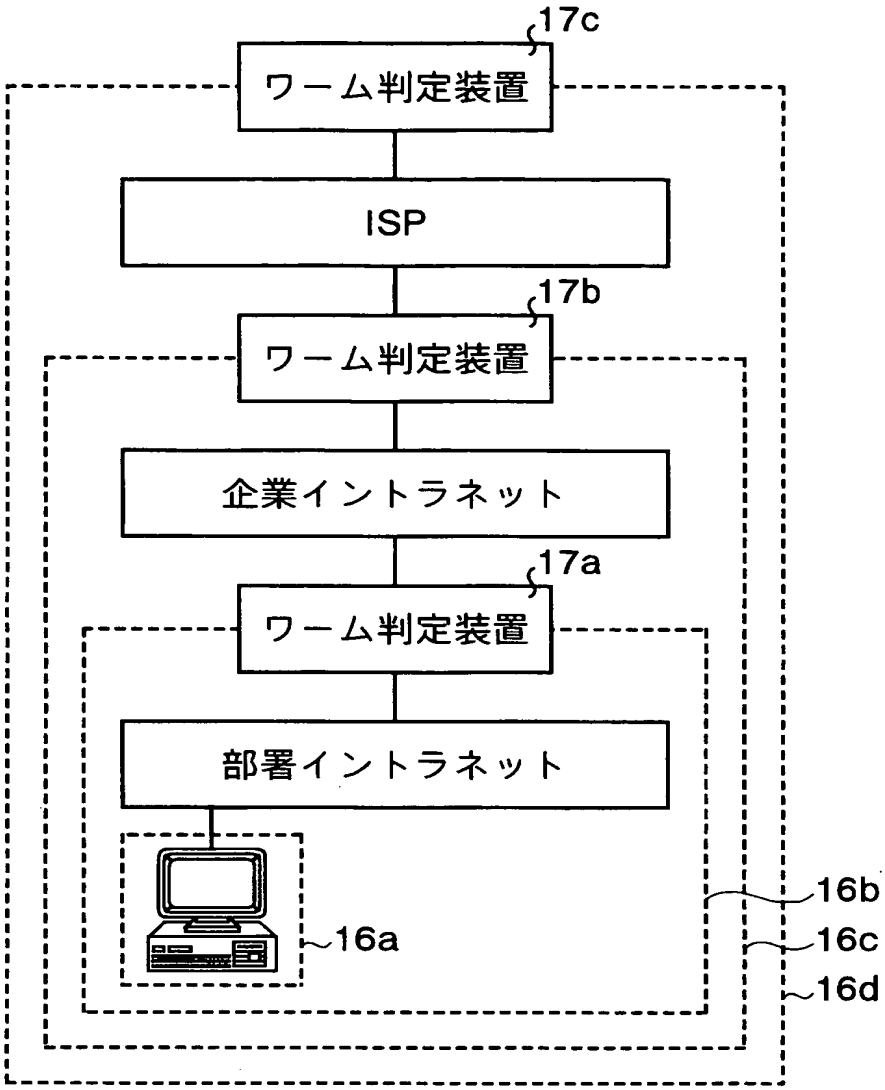
【図１５－２】

図14に示した状況判定処理の処理手順を示すフローチャート(2)



【図１６】

ネットワークセグメントの概念を説明する概念図



【書類名】要約書
【要約】
【課題】サーバ装置かクライアント装置かに拘らず通信がワームによりなされたものか否かを容易にかつ効率的に判定すること。
【解決手段】通信情報取得部２４０ａが、設定データ２３０ａに記憶された情報の取得に係る設定情報に基づいて通信パケットの通信量および通信パケットの通信アドレスに係る情報を取得し、ワーム判定部２４０ｂが、通信情報取得部２４０ａにより取得された情報および通信がワームによりなされた通信か否かを規定する、設定データ２３０ａに記憶された判定基準に係る情報に基づいて、通信がワームによりなされた通信か否かを判定する。
【選択図】　図２

特願２００３－３６７２７２

出　願　人　履　歴　情　報

識別番号　［０００００５２２３］

１．変更年月日　１９９６年　３月２６日
［変更理由］　住所変更
住　所　神奈川県川崎市中原区上小田中４丁目１番１号
氏　名　富士通株式会社